



JUNOS™
Internet Software
Configuration Guide

Getting Started

Release 5.4

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-007533-01, Revision 1

NETWORKS
juniper

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., Copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks is registered in the U.S. Patent and Trademark Office and in other countries as a trademark of Juniper Networks, Inc. Broadband Cable Processor, G10, Internet Processor, JUNOS, JUNOScript, M5, M10, M20, M40, M40e, M160, M-series, T320, T640, and T-series are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

JUNOS Internet Software Configuration Guide: Getting Started, Release 5.4
Copyright © 2002, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writers: Margaret Jones, John Gilbert Chan
Editor: Cathy Steinberg
Covers and template design: Edmonds Design

Revision History
8 July 2002—First Edition.

The information in this document is current as of the date listed in the revision history above.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer or otherwise revise this publication without notice.

Juniper Networks reserves the right to change, modify, transfer or otherwise revise this publication without notice.

Products made or sold by Juniper Networks (including the G10 CMTS, the M5 router, the M10 router, the M20 router, the M40 router, the M40e router, the M160 router, the T320 router, the T640 routing node, and the JUNOS software) or components thereof may be covered by one or more of the following patents which are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

Abbreviated Table of Contents

About this Manual

Part 1

Overview

Chapter 1	Product Architecture	3
Chapter 2	JUNOS Software Overview	9
Chapter 3	Complete Configuration Mode Commands and Statements	33

Part 2

Software Installation and Upgrade

Chapter 4	Installation Overview	75
Chapter 5	Configure the Software Initially	81
Chapter 6	Reinstall the Software	85

Chapter 7	Upgrade Software Packages	89
-----------	---------------------------------	----

Chapter 8	Upgrade to Release 5.0 or Downgrade from Release 5.0	95
-----------	--	----

Part 3

Command-Line Interface

Chapter 9	Command-Line Interface Overview	101
-----------	---------------------------------------	-----

Chapter 10	Command-Line Interface Operational Mode	103
------------	---	-----

Chapter 11	Control the CLI Environment	123
------------	-----------------------------------	-----

Chapter 12	Configure the Router with the CLI	127
------------	---	-----

Chapter 13	Configuration Groups	179
------------	----------------------------	-----

Chapter 14	Summary of CLI Environment Commands	197
------------	---	-----

Chapter 15	Summary of CLI Configuration Mode Commands	203
------------	--	-----

Chapter 16	Summary of CLI Operational Mode Commands	215
------------	--	-----

Part 4

System Management

Chapter 17	System Management Overview	223
Chapter 18	System Management Configuration Statements.....	229
Chapter 19	Configure Basic System Management.....	233
Chapter 20	Configure System Authentication.....	241
Chapter 21	Configure User Access	253
Chapter 22	Configure Time.....	265
Chapter 23	Configure System Logging.....	271
Chapter 24	Configure Miscellaneous System Management Features	277
Chapter 25	Summary of System Management Configuration Statements.....	285

Part 5

Access

Chapter 26	Access Configuration Guidelines	321
------------	---------------------------------------	-----

Part 6

Security Services

Chapter 27

Security Services Overview..... 329

Chapter 28

Security Services Configuration Guidelines..... 333

Chapter 29

Summary of Security Services
Configuration Statements 361

Part 7

Router Chassis

Chapter 30

Router Chassis Configuration Guidelines 379

Chapter 31

Summary of Router Chassis Configuration Statements..... 397

Part 8

Appendix

Appendix A

Glossary..... 413

Part 9

Index

Index

Index 435

Index

Index of Statements and Commands 451

Table of Contents

About this Manual

Objectives	xxvii
Audience.....	xxviii
Document Organization.....	xxviii
Part Organization.....	xxx
Using the Indexes	xxxi
Documentation Conventions	xxxii
General Conventions	xxxii
Conventions for Software Commands and Statements	xxxii
List of Technical Publications	xxxiv
Documentation Feedback	xxxv
How to Request Support	xxxv

Part 1

Overview

Chapter 1

Product Architecture	3
----------------------------	---

Hardware Overview	3
Product Architecture	4
Packet Forwarding Engine	5
Packet Flow through an M-Series Router	5
Packet Flow through a T-series Router.....	6
Routing Engine	7

Chapter 2

JUNOS Software Overview	9
-------------------------------	---

Routing Engine Software Components.....	9
Routing Protocol Process	10
Routing Protocols (IPv4)	10
Routing Protocols (IPv6)	12
Routing and Forwarding Tables.....	12
Routing Policy	13

VPNs	14
Interface Process	14
Chassis Process	14
SNMP and MIB II Processes	14
Management Process	15
Routing Engine Kernel.....	15
Software Installation Overview	15
Tools for Accessing and Controlling the Software	15
Software Configuration Overview	16
Methods of Configuring the Software	16
Configuring the Software.....	16
Activating a Configuration	17
Software Monitoring Tools.....	17
Router Security	17
JUNOS Default Settings.....	18
Router Access.....	19
User Authentication.....	19
Routing Protocol Security Features.....	20
Firewall Filters.....	20
Auditing for Security.....	20
Supported Software Standards.....	21
Supported Internet RFCs and Drafts	21
ATM	21
BGP	21
CHAP	22
Frame Relay.....	22
GMPLS.....	22
GRE and IP-IP Encapsulation.....	23
IP Multicast	23
IPSec and IKE.....	23
IPv6.....	24
IS-IS.....	25
LDP	25
MIBs	26
MPLS.....	28
OSPF.....	28
PPP	29
RIP	29
RSVP	29
SSL.....	29
TCP/IP v4	30
Supported ISO Standards.....	31
IS-IS.....	31
Supported SDH and SONET Standards	31
Other Supported Standards	32
ATM	32
Ethernet	32
Frame Relay.....	32
T3	32

Chapter 3

Complete Configuration Mode

Commands and Statements 33

Complete Configuration Mode Commands 33

Complete Configuration Statement Hierarchy 34

[edit access] Hierarchy Level 35

[edit accounting-options] Hierarchy Level 35

[edit chassis] Hierarchy Level 36

[edit class-of-service] Hierarchy Level 37

[edit firewall] Hierarchy Level 38

[edit forwarding-options] Hierarchy Level 38

[edit groups] Hierarchy Level 40

[edit interfaces] Hierarchy Level 41

[edit policy-options] Hierarchy Level 46

[edit protocols] Hierarchy Level 46

[edit routing-instances] Hierarchy Level 60

[edit routing-options] Hierarchy Level 63

[edit security] Hierarchy Level 66

[edit snmp] Hierarchy Level 67

[edit system] Hierarchy Level 69

Part 2

Software Installation and Upgrade

Chapter 4

Installation Overview 75

JUNOS Software Distribution 75

Software Release Names 76

Package Names 76

Storage Media 78

Boot Devices 78

Boot Sequence 79

Chapter 5

Configure the Software Initially 81

Chapter 6

Reinstall the Software 85

Prepare to Reinstall the JUNOS Software 85

Reinstall the JUNOS Software 85

Reconfigure the JUNOS Software 86

Chapter 7	Upgrade Software Packages	89
	Upgrade All Software Packages.....	90
	Upgrade Individual Software Packages	93
Chapter 8	Upgrade to Release 5.0 or Downgrade from Release 5.0.....	95
Part 3	Command-Line Interface	
Chapter 9	Command-Line Interface Overview	101
	CLI Modes.....	101
	CLI Command Hierarchy	102
Chapter 10	Command-Line Interface Operational Mode.....	103
	Use the CLI	104
	Get Help About Commands	105
	Examples: Get Help About Commands.....	105
	Have the CLI Complete Commands.....	106
	Examples: Use CLI Command Completion	107
	CLI Messages	107
	Move around and Edit the Command Line	108
	How Output Appears on the Screen	109
	Display Output One Screen at a Time	109
	Filter Command Output	110
	Place Command Output in a File.....	111
	Search for a String in the Output.....	112
	Compare Configuration Changes with a Prior Version.....	114
	Count the Number of Lines in the Output	116
	Display All Output at Once.....	116
	Retain the Output after the Last Screen.....	116
	Display Additional Information about the Configuration	116
	Filter Command Output Multiple Times	119
	Set the Current Date and Time	119
	Set Date and Time from NTP Servers	119
	Display CLI Command History.....	120
	Monitor Who Uses the CLI	121

Chapter 11

Control the CLI Environment 123

Set the Terminal Type.....	124
Set the Screen Length	124
Set the Screen Width	124
Set the CLI Prompt.....	124
Set the Idle Timeout.....	124
Set CLI to Prompt after a Software Upgrade.....	125
Set Command Completion.....	125
Display CLI Settings	125
Example: Control the CLI Environment.....	125

Chapter 12

Configure the Router with the CLI..... 127

Configuration Statement Hierarchy.....	128
How the Configuration Is Stored	130
Enter Configuration Mode.....	131
Using the Configure Command.....	132
Using the Configure Exclusive Command	132
Using the Configure Private Command.....	133
Update the Configure Private Configuration	135
Configuration Mode Prompt.....	136
Configuration Mode Banner	136
Configuration Statements and Identifiers.....	136
Get Help about Configuration Mode Commands,	
Statements, and Identifiers.....	139
Use Command Completion in Configuration Mode.....	139
Examples: Use Command Completion in Configuration Mode	139
Get Help Based on a String in a Statement Name	141
Example: Get Help Based on a String Contained in a	
Statement Name	141
Create and Modify the Configuration	142
Examples: Create and Modify the Configuration.....	143
Move among Levels of the Hierarchy	145
Move Down to a Specific Level	146
Move Back Up to Your Previous Level.....	146
Move Up One Level	146
Move Directly to the Top of the Hierarchy	147
Warning Messages When Moving Up.....	147
Issue Relative Configuration Commands	147
Exit Configuration Mode	148
Display the Current Configuration.....	148
Examples: Display the Current Configuration	149
Display Users Currently Editing the Configuration	150
Remove a Statement from the Configuration.....	150
Examples: Remove a Statement from the Configuration	151
Copy a Statement in the Configuration	152
Example: Copy a Statement in the Configuration	152
Rename an Identifier	153
Example: Rename an Identifier	153

Insert a New Identifier	153
Examples: Insert a New Identifier.....	154
Run an Operational Mode CLI Command from Configuration Mode.....	156
Example: Run an Operational Mode CLI Command from Configuration Mode.....	156
Display Configuration Mode Command History.....	156
Verify a Configuration.....	157
Commit a Configuration	157
Commit a Configuration and Exit Configuration Mode	158
Activate a Configuration but Require Confirmation	158
Synchronize Routing Engines	160
Example: Apply Groups Re0 and Re1	160
Example: Set Apply Groups Re0 and Re1	161
Save a Configuration to a File	161
Load a Configuration	162
Examples: Load a Configuration from a File	163
Return to a Previously Committed Configuration.....	164
Example: Return to a Previously Committed Version of the Configuration ..	165
Configuration Mode Error Messages	165
Deactivate and Reactivate Statements and Identifiers in a Configuration	166
Examples: Deactivate and Reactivate Statements and Identifiers in a Configuration.....	167
Add Comments in a Configuration.....	167
Examples: Include Comments in Configurations	168
Have Multiple Users Configure the Software	170
Example: Using the CLI to Configure the Router	170
Shortcut.....	170
Longer Configuration Example	170
Additional Details about Specifying Statements and Identifiers	176
How to Specify Statements	176
How the CLI Performs Type-Checking	178

Chapter 13 Configuration Groups

Overview	179
Inheritance Model	180
Configuration Groups Configuration Statements	180
Configuration Groups Configuration Guidelines	180
Create a Configuration Group	181
Apply a Configuration Group	181
Example: Configure and Apply Configuration Groups.....	182
Display Inherited Values.....	183
Use Wildcards	184
Example: Use Wildcards.....	186
Examples: Configuration Groups	187
Configure Sets of Statements.....	187
Configure Interfaces	189
Configure Peer Entities	191
Establish Regional Configurations.....	193
Select Wildcard Names.....	194
Summary of Configuration Group Statements	195
apply-groups.....	195
groups	196

Chapter 14

Summary of CLI Environment Commands.....197

set cli complete-on-space.....	197
set cli idle-timeout	198
set cli prompt.....	198
set cli restart-on-upgrade	198
set cli screen-length	199
set cli screen-width	199
set cli terminal	199
set date.....	200
set date ntp	200
show cli	200
show cli history.....	201

Chapter 15

Summary of CLI Configuration Mode Commands203

activate	203
annotate	204
commit.....	205
copy.....	206
deactivate	206
delete	207
edit	207
exit	208
help	208
insert	209
load	209
quit.....	210
rename	210
rollback.....	211
run.....	211
save	212
set.....	213
show.....	213
status	213
top.....	214
up	214

Chapter 16

Summary of CLI Operational Mode Commands.....215

clear.....	215
configure	215
file	215
monitor	216
ping	216
update	216
(pipe).....	217
quit.....	217

request	218
restart	218
set	218
show.....	218
ssh.....	219
start.....	219
telnet.....	219
test	219
traceroute	219

Part 4 System Management

Chapter 17	System Management Overview.....	223
------------	---------------------------------	-----

How to Specify IP Addresses, Network Masks, and Prefixes	223
How to Specify Filenames and URLs.....	224
Directories on the Router	225
Tracing and Logging Operations	225
Protocol Authentication	226
User Authentication	227

Chapter 18	System Management Configuration Statements	229
------------	--	-----

Chapter 19	Configure Basic System Management.....	233
------------	--	-----

Configure the Router's Name and Addresses	233
Configure the Router's Name	233
Map the Router's Name to IP Addresses	234
Configure an ISO Sysid.....	234
Example: Configure a Router's Name, IP Address, and Sysid	235
Configure the Router's Domain Name	235
Example: Configure the Router's Domain Name	235
Configure Which Domains to Search	236
Example: Configure Which Domains to Search	236
Configure a DNS Name Server.....	236
Example: Configure a DNS Name Server	236
Configure a Backup Router	237
Example: Configure a Backup Router	237
Configure Flash Disk Mirroring	238
Configure the System Location	238
Configure the Root Password.....	239
Example: Configure the Root Password.....	239
Compress the Current Configuration File	240

Chapter 20

Configure System Authentication.....241

Configure RADIUS Authentication	241
Configure Juniper Networks-Specific RADIUS Attributes	242
Configure TACACS+ Authentication	243
Configure Juniper Networks-Specific TACACS+ Attributes	244
Configure Template Accounts for RADIUS and TACACS+ Authentication	245
Remote Template Accounts.....	245
Local User Template Accounts.....	246
Local User Template Example:	246
Configure the Authentication Order	248
Example: Remove an Ordered Set from the Authentication Order	248
Example: Insert an Order Set in the Authentication Order.....	248
Examples: Configure System Authentication	249
Local User Fallback Mechanism.....	250
Example 1: Insert Password into the Authentication Order	251
Example 2: Default to Local User Password Authentication, TACACS +	251
Example 3: Default to Local User Password Authentication, RADIUS	251
Example 4: Default to Local User Password Authentication, TACACS + and RADIUS.....	252

Chapter 21

Configure User Access253

Define Login Classes	253
Configure Access Privilege Levels	254
Example: Configure Access Privilege Levels	256
Deny or Allow Individual Commands	256
Operational Mode Commands.....	257
Example 1: Define Access Privileges to Individual Operational Mode Commands	258
Configuration Mode Commands.....	259
Example 3: Define Access Privileges to Individual Configuration Mode Commands	261
Example 4: Configure Access Privileges to Individual Configuration Mode Commands	261
Configure the Timeout Value for Idle Login Sessions	262
Configure User Accounts	262
Example: Configure User Accounts.....	264

Chapter 22

Configure Time 265

Set the Time Zone	265
Examples: Set the Time Zone	265
Configure the Network Time Protocol.....	266
Configure the NTP Boot Server	267
Configure the NTP Time Server and Time Services.....	267
Configure the Router to Operate in Client Mode.....	268
Configure the Router to Operate in Symmetric Active Mode	268
Configure the Router to Operate in Broadcast Mode	269
Configure NTP Authentication Keys	269
Configure the Router to Listen for Broadcast Messages	270
Configure the Router to Listen for Multicast Messages.....	270

Chapter 23

Configure System Logging 271

Configure System Logging	271
Archive System Logs.....	273
Override the Facility	274
Configure Log Message Prefixes	275
Examples: Configure System Logging	275

Chapter 24

Configure Miscellaneous System Management Features 277

Configure Console and Auxiliary Port Properties	277
Disable the Sending of Redirect Messages on the Router	278
Configure the Source Address for Locally Generated TCP/IP Packets	278
Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent	279
Configure System Services.....	280
Configure Finger Service	280
Configure FTP Service	281
Configure rlogin Service	281
Configure ssh Service	281
Configure Root Login.....	282
Configure ssh Protocol Version.....	282
Configure telnet Service	283
Configure a System Login Message.....	283
Configure JUNOS Software Processes	283
Disable JUNOS Software Processes	283
Configure Failover to Backup Media if a Software Process Fails	284
Configure a Password on the Diagnostics Port.....	284
Core Dump Files.....	284

Summary of System Management Configuration Statements

allow-commands	285
allow-configuration	286
authentication.....	286
authentication-key	287
authentication-order	287
auxiliary	288
backup-router	288
boot-server	289
broadcast.....	289
broadcast-client	290
class.....	290
compress-configuration-files	291
console	291
default-address-selection.....	292
deny-commands.....	292
deny-configuration.....	293
dhcp-relay.....	294
diag-port-authentication.....	295
domain-name	295
domain-search.....	296
full-name	296
host-name.....	296
idle-timeout	297
interface	298
load-key-file	298
location.....	299
login	300
message.....	300
mirror-flash-on-disk	301
multicast-client	301
name-server.....	302
no-redirects.....	302
no-saved-core-context.....	302
ntp.....	303
peer	303
permissions	304
port.....	304
ports	304
processes.....	305
protocol-version.....	306
radius-server.....	306
retry.....	307
root-authentication	307
root-login	308
secret.....	308
server	309
services.....	310
single-connection.....	311
static-host-mapping	311
syslog.....	312
system.....	313

tacplus-server	314
timeout	314
time-zone	315
trusted-key	317
uid	317
user	318

Part 5 Access

Chapter 26

Access Configuration Guidelines	321
---------------------------------------	-----

Configure Challenge Handshake Authentication Protocol.....	322
Example: PPP Challenge Handshake Authentication Protocol.....	322
Configure the Authentication Order	323
Trace Access Processes.....	324
Summary of Access Configuration Statements	325
authentication-order	325
profile	325
traceoptions.....	326

Part 6 Security Services

Chapter 27

Security Services Overview.....	329
---------------------------------	-----

IPSec Overview.....	329
Security Associations	330
IPSec Security	330
Host-to-Host Protection	330
Gateway-to-Gateway Protection.....	330
IKE	331

Minimum IPSec Configuration	335
Minimum Manual SA Configuration	335
Minimum Dynamic SA Configuration	335
Configure Global IPSec Properties	336
Configure IPSec Proposal Properties	336
Configure Security Associations	337
IPSec Security	337
Host-to-Host Security	338
Gateway-to-Gateway Security	338
Configure IPSec Mode	338
Configure Manual Security Associations	339
Configure Direction	340
Configure the Protocol	341
Configure a Security Parameter Index (SPI)	341
Configure Authentication	341
Configure Encryption	342
Configure Dynamic Security Associations	343
Configure IKE (Dynamic SAs Only)	344
IKE Global Properties	344
IKE Proposal Properties	344
Configure an IKE Proposal	345
Configure an IKE Authentication Algorithm	345
Configure an IKE Authentication Method	345
Configure an IKE Diffie-Hellman Group	346
Configure an IKE Encryption Algorithm	346
Configure IKE Lifetime	346
Example: IKE Proposal Configuration	347
Configure an IKE Policy	347
Configure IKE Policy Mode	348
Configure IKE Policy Proposal	348
Configure IKE Policy Preshared Key	348
Example: Configure IKE Policy	349
Configure an IPSec Proposal	350
Configure an Authentication Algorithm	350
Configure an Encryption Algorithm	350
Configure IPSec Lifetime	351
Configure Protocol for Dynamic SA	351
Configure an IPSec Policy	352
Configure Perfect Forward Secrecy	352
Example: IPSec Policy Configuration	353
Configure Traceoptions	354
Configure the ES PIC	354
Example: ES PIC Configuration	355
Configure Traffic	355
Traffic Overview	356
Example 1: Configure Outbound Traffic Filter	357
Example 2: Apply Outbound Traffic Filter	358
Example 3: Configure Inbound Traffic Filter for Policy Check	358
Example 4: Apply Inbound Traffic Filter to ES PIC for Policy Check	359
Configure an ES Tunnel Interface for a Layer 3 VPN	360
Configure JUNOScript XML-SSL Service	360

Chapter 29

Summary of Security Services

Configuration Statements 361

authentication.....	361
authentication-algorithm.....	362
authentication-algorithm (IKE).....	362
authentication-algorithm (IPSec).....	362
authentication-method	363
certificates	363
dh-group.....	363
direction	364
dynamic	364
encryption	365
encryption-algorithm	366
ike	366
ipsec.....	367
lifetime-seconds.....	368
manual	368
mode	369
mode (IPSec)	369
mode (IKE)	369
perfect-forward-secrecy	370
policy.....	370
policy (IPSec).....	370
policy (IKE).....	371
pre-shared-key.....	371
proposal	372
proposal (IKE).....	372
proposal (IPSec).....	372
protocol.....	373
protocol (manual SA)	373
protocol (dynamic SA)	373
security-association	374
spi	374
traceoptions.....	375

Part 7

Router Chassis

Chapter 30

Router Chassis Configuration Guidelines 379

Minimum Chassis Configuration.....	380
Configure Aggregated Devices	381
Configure ATM Cell-Relay Accumulation Mode	381
Configure Conditions That Trigger Alarms	382
Chassis Conditions That Trigger Alarms	383
Silence External Devices	384
Configure SONET/SDH Framing	384
Configure Sparse DLCIS Mode	385

Configure Channelized PIC Operation	385
Concatenated and Nonconcatenated Mode.....	386
Channelized DS-3 to DS-0 Naming.....	386
Channelized E1 Naming.....	388
Channelized STM-1 Interface Virtual Tributary Mapping	389
Configure the Drop Policy for Traffic with Source-Route Constraints	390
Configure Redundancy	390
Configure Routing Engine Redundancy	390
Copy a Configuration File from One Routing Engine to the Other	391
Load a Package from the Other Routing Engine	393
Change over to the Backup Routing Engine	393
Configure SFM Redundancy.....	394
Configure SSB Redundancy	394
Configure Packet Scheduling.....	395

Chapter 31

Summary of Router Chassis Configuration Statements.....397

aggregated-devices	397
alarm	398
atm-cell-relay-accumulation	398
ce1	399
channel-group.....	399
chassis	399
ct3	400
device-count	400
e1	400
ethernet.....	401
failover on-loss-of keepalives	401
fpc	402
framing	403
keepalive-time	403
no-concatenate	404
packet-scheduling	404
pic	405
port.....	405
redundancy	406
routing-engine	406
sfm	407
sonet.....	407
source-route	408
ssb	408
sparse-dlcis	409
t1	409
timeslots.....	409
vtmapping	410

Part 8

Appendix

Appendix A

Glossary 413

Part 9

Index

Index

Index 435

Index

Index of Statements and Commands 451

List of Figures

List of Figures

Figure 1:	Product Architecture	5
Figure 2:	CLI Command Hierarchy Example.....	102
Figure 3:	Configuration Mode Hierarchy of Statements	129
Figure 4:	Commands for Storing and Modifying the Router Configuration.....	130
Figure 5:	Confirm a Configuration	159
Figure 6:	Example 1: Load a Configuration from a File.....	163
Figure 7:	Example 2: Load a Configuration from a File.....	163
Figure 8:	Example 3: Load a Configuration from a File.....	164
Figure 9:	Example: IPSec Tunnel Connecting Security Gateways	356

List of Figures

List of Tables

List of Tables

Table 1:	Juniper Networks Technical Documentation	xxxiv
Table 2:	Release 5.x Device Names	78
Table 3:	CLI Keyboard Sequences	108
Table 4:	---More--- Prompt Keyboard Sequences	109
Table 5:	Common Regular Expression Operators	112
Table 6:	Configuration Mode Top-Level Statements	137
Table 7:	CLI Configuration Input Types	178
Table 8:	Juniper Networks-Specific RADIUS Attributes	242
Table 9:	Juniper Networks-Specific TACACS+ Attributes	244
Table 10:	Login Class Permission Bits	255
Table 11:	Default System Login Classes	256
Table 12:	Operational Mode Commands—Common Regular Expression Operators	258
Table 13:	Configuration Mode Commands—Common Regular Expression Operators	260
Table 14:	System Logging Facilities	272
Table 15:	System Logging Severity Levels	273
Table 16:	System Logging Facilities That You Can Specify on the facility-override Statement	274
Table 17:	Configurable PIC Alarm Conditions	382
Table 18:	Chassis Component Alarm Conditions	383
Table 19:	Ranges for Channelized DS-3 to DS-0 Configuration	387
Table 20:	Ranges for Channelized E1 Configuration	389

About this Manual

This chapter provides a high-level overview of the *JUNOS Internet Software Configuration Guide: Getting Started*.

- Objectives on page xxvii
- Audience on page xxviii
- Document Organization on page xxviii
- Part Organization on page xxx
- Using the Indexes on page xxxi
- Documentation Conventions on page xxxii
- List of Technical Publications on page xxxiv
- Documentation Feedback on page xxxv
- How to Request Support on page xxxv

Objectives

This manual provides an overview of the JUNOS Internet software and describes how to install and upgrade the software. This manual also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.

This manual documents Release 5.4 of the JUNOS Internet software. To obtain additional information about the JUNOS software—either corrections to information in this manual or information that might have been omitted from this manual—refer to the software release notes.

To obtain additional information about the JUNOS software—either corrections to information in this manual or information that might have been omitted from this manual—refer to the printed software release notes that accompany your router.

To obtain the most current version of this manual and the most current version of the software release notes, refer to the product documentation page on the Juniper Networks Web site, which is located at <http://www.juniper.net/>.

To order printed copies of this manual or to order a documentation CD-ROM, which contains this manual, please contact your sales representative.

Audience

This manual is designed for network administrators who are configuring a Juniper Networks router. It assumes that you have a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. This manual assumes that you are familiar with one or more of the following Internet routing protocols: Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Internet Control Message Protocol (ICMP) router discovery, Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), Protocol-Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), Routing Information Protocol (RIP), and Simple Network Management Protocol (SNMP).

Document Organization

This manual is divided into several parts. Each part describes a major functional area of the JUNOS software, and the individual chapters within a part describe the software components of that functional area.

This manual contains the following parts and chapters:

- Preface, “About this Manual” (this chapter), provides a brief description of the contents and organization of this manual and describes how to contact customer support.
- Part 1, “Overview,” provides an overview of the hardware and software components of the router, describes the user command-line interface, and provides the procedures for installing and upgrading the software.
 - Chapter 1, “Product Architecture,” discusses the router hardware and product architecture.
 - Chapter 2, “JUNOS Software Overview,” provides an overview of the JUNOS software features and lists the software standards that the JUNOS software supports.
 - Chapter 3, “Complete Configuration Mode Commands and Statements,” lists all the commands available in configuration mode. It also lists the complete configuration statement hierarchy, showing all possible configuration statements and levels in the configuration hierarchy.
- Part 2, “Software Installation and Upgrade,” describes how to install, reinstall, and upgrade the JUNOS software on a router.
 - Chapter 4, “Installation Overview,” provides background information for the installation process.
 - Chapter 5, “Configure the Software Initially,” describes how to initially configure the JUNOS software.

- Chapter 6, “Reinstall the Software,” describes how to reinstall the JUNOS software.
- Chapter 7, “Upgrade Software Packages,” describes how to upgrade software packages.
- Chapter 8, “Upgrade to Release 5.0 or Downgrade from Release 5.0,” describes how to upgrade to Release 5.0 or downgrade from Release to 5.0.
- Part 3, “Command-Line Interface,” describes the interface that you use to configure and monitor the JUNOS software. The command-line interface (CLI) is the interface you use when you access the router.
 - Chapter 9, “Command-Line Interface Overview,” provides an overview of the functions of the CLI.
 - Chapter 10, “Command-Line Interface Operational Mode,” describes the operational mode of the CLI.
 - Chapter 11, “Control the CLI Environment,” describes how to configure the CLI environment.
 - Chapter 12, “Configure the Router with the CLI,” describes the configuration mode of the CLI.
 - Chapter 13, “Configuration Groups,” describes configuration groups.
 - Chapter 14, “Summary of CLI Environment Commands,” explains each of the CLI environment commands.
 - Chapter 15, “Summary of CLI Configuration Mode Commands,” explains each of the CLI configuration mode commands.
 - Chapter 16, “Summary of CLI Operational Mode Commands,” explains each of the CLI operational mode commands.
- Part 4, “System Management,” describes how to use the CLI to manage the router.
 - Chapter 17, “System Management Overview,” provides background information for configuring system management functions.
 - Chapter 18, “System Management Configuration Statements,” lists all the statements available at the [edit system] hierarchy level.
 - Chapter 19, “Configure Basic System Management,” describes how to configure basic system management functions.
 - Chapter 20, “Configure System Authentication,” describes how to configure RADIUS and TACACS+ authentication.
 - Chapter 21, “Configure User Access,” describes how to configure user access.
 - Chapter 22, “Configure Time,” describes how to set the time zone and configure the Network Time Protocol, which provides mechanisms to synchronize time and coordinate time distribution in a large, diverse network.
 - Chapter 23, “Configure System Logging,” describes how to control system logging and how much information the system should log.

- Chapter 24, “Configure Miscellaneous System Management Features,” describes how to configure various system management functions, such as console and auxiliary port properties and the source address for locally generated TCP/IP packets.
- Chapter 25, “Summary of System Management Configuration Statements,” explains each of the system management configuration statements.
- Part 5, “Access,” describes how to configure access services.
 - Chapter 26, “Access Configuration Guidelines,” describes how to configure access and explains each of the access configuration statements.
- Part 6, “Security Services,” describes how to configure security services.
 - Chapter 27, “Security Services Overview,” provides background information for configuring security services.
 - Chapter 28, “Security Services Configuration Guidelines,” describes how to configure security service properties.
 - Chapter 29, “Summary of Security Services Configuration Statements,” explains each of the security services configuration statements.
- Part 7, “Router Chassis,” covers the configuration of router chassis properties.
 - Chapter 30, “Router Chassis Configuration Guidelines,” describes how to configure router chassis properties.
 - Chapter 31, “Summary of Router Chassis Configuration Statements,” provides a detailed listing of all configuration statements used in router chassis configuration.

This manual also contains a glossary, a complete index, and an index of statements and commands.

Part Organization

The parts in this manual generally include the following information:

- Overview—Provides background information about and discusses concepts related to the software component described in that part of the book.
- Configuration statements—Lists all the configuration statements available to configure the software component. This list is designed to provide an overview of the configuration statement hierarchy for that software component.
- Configuration guidelines—Describes how to configure all the features of the software component. The first section of the configuration guidelines describes the minimum configuration for that component, listing the configuration statements you must include to enable the software component on the router with only the bare minimum functionality. The remaining sections in the configuration guidelines are generally arranged so that the most common features are near the beginning.

- **Statement summary**—A reference that lists all configuration statements alphabetically and explains each statement and all its options. The explanation of each configuration statement consists of the following parts:
 - **Syntax**—Describes the full syntax of the configuration statement. For an explanation of how to read the syntax statements, see “Documentation Conventions” on page xxxii.
 - **Hierarchy level**—Tells where in the configuration statement hierarchy you include the statement.
 - **Description**—Describes the function of the configuration statement.
 - **Options**—Describes the configuration statement’s options, if there are any. For options with numeric values, the allowed range and default value, if any, are listed. For multiple options, the default is stated. If a configuration statement is at the top of a hierarchy of options that are other configuration statements, these options are generally explained separately in the statement summary section.
 - **Usage guidelines**—Points to the section or sections in the configuration guidelines section that describe how to use the configuration statement.
 - **Required privilege level**—Indicates the permissions that the user must have to view or modify the statement in the router configuration. For an explanation of the permissions, see the appropriate chapters in this manual.
 - **See also**—Indicates other configuration statements that might provide related or similar functionality.

Using the Indexes

This manual contains two indexes: a complete index, which contains all index entries, and an index that contains only statements and commands.

In the complete index, bold page numbers point to pages in the statement summary chapters. The index entry for each configuration statement always contains at least two entries. The first, with a bold page number on the same line as the statement name, references the statement summary section. The second entry, “usage guidelines,” references the section in a configuration guidelines chapter that describes how to use the statement.

Documentation Conventions

General Conventions

This manual uses the following text conventions:

- Statements, commands, filenames, directory names, IP addresses, and configuration hierarchy levels are shown in a sans serif font. In the following example, *stub* is a statement name and [edit protocols ospf area *area-id*] is a configuration hierarchy level:

To configure a stub area, include the stub statement at the [edit protocols ospf area *area-id*] hierarchy level:

- In examples, text that you type literally is shown in bold. In the following example, you type the word *show*:

```
[edit protocols ospf area area-id]  
cli# show  
stub <default-metric metric>
```

- Examples of command output are generally shown in a fixed-width font to preserve the column alignment. For example:

```
> show interfaces terse  
Interface      Admin Link Proto Local              Remote  
at-1/3/0       up    up  
at-1/3/0.0     up    up    inet  1.0.0.1            --> 1.0.0.2  
               iso  
fxp0           up    up  
fxp0.0         up    up    inet  192.168.5.59/24
```

Conventions for Software Commands and Statements

When describing the JUNOS software, this manual uses the following type and presentation conventions:

- Statement or command names that you type literally are shown nonitalicized. In the following example, the statement name is *area*:

You configure all these routers by including the following area statement at the [edit protocols ospf] hierarchy level:

- Options, which are variable terms for which you substitute appropriate values, are shown in italics. In the following example, *area-id* is an option. When you type the area statement, you substitute a value for *area-id*.

```
area area-id;
```

- Optional portions of a configuration statement are enclosed in angle brackets. In the following example, the “default-metric *metric*” portion of the statement is optional:

```
stub <default-metric metric>;
```


- For text strings separated by a pipe (|), you must specify either *string1* or *string2*, but you cannot specify both or neither of them. Parentheses are sometimes used to group the strings.

```
string1 | string2
(string1 | string2)
```

In the following example, you must specify either broadcast or multicast, but you cannot specify both:

```
broadcast | multicast
```

- For some statements, you can specify a set of values. The set must be enclosed in square brackets. For example:

```
community name members [community-id]
```

- The configuration examples in this manual are generally formatted in the way that they appear when you issue a show command. This format includes braces ({ }) and semicolons. When you type configuration statements in the CLI, you do not type the braces and semicolons. However, when you type configuration statements in an ASCII file, you must include the braces and semicolons. For example:

```
[edit]
cli# set routing-options static route default nexthop address retain
[edit]
cli# show
routing-options {
  static {
    route default {
      nexthop address;
      retain;
    }
  }
}
```

- Comments in the configuration examples are shown either preceding the lines that the comments apply to, or more often, they appear on the same line. When comments appear on the same line, they are preceded by a pound sign (#) to indicate where the comment starts. In an actual configuration, comments can only precede a line; they cannot be on the same line as a configuration statement. For example:

```
protocols {
  mpls {
    interface (interface-name | all); # Required to enable MPLS on the interface
  }
  rsvp {
    interface interface-name; # Required for dynamic MPLS only
  }
}
```

- The general syntax descriptions provide no indication of the number of times you can specify a statement, option, or keyword. This information is provided in the text of the statement summary.

List of Technical Publications

Table 1 lists the software and hardware books for Juniper Networks routers and describes the contents of each book.

Table 1: Juniper Networks Technical Documentation

Book	Description
JUNOS Internet Software Configuration Guides	
<i>Getting Started</i>	Provides an overview of the JUNOS Internet software and describes how to install and upgrade the software. This manual also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.
<i>Interfaces and Class of Service</i>	Provides an overview of the interface and class-of-service functions of the JUNOS Internet software and describes how to configure the interfaces on the router.
<i>IPv6</i>	Provides an overview of IPv6 concepts such as addressing and packet header structure, and discusses the differences between IPv4 and IPv6. This manual also describes how to configure IPv6 on a router and discusses transition from IPv4 to IPv6.
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP, accounting options, and cflowd.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Routing and Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>VPNs</i>	Provides an overview of Layer 2 and Layer 3 Virtual Private Networks (VPNs), describes how to configure VPNs, and provides configuration examples.
JUNOS Internet Software Command Reference	
<i>Operational Mode Command Reference</i>	Describes the JUNOS Internet software operational mode commands you use to monitor and troubleshoot Juniper Networks routers.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
JUNOScript API Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript API to monitor and configure Juniper Networks routers.
<i>JUNOScript API Reference</i>	Provides a reference page for each tag in the JUNOScript API.
JUNOS Internet Software Comprehensive Index	
<i>Comprehensive Index</i>	Provides a complete index of all JUNOS Internet software books and the <i>JUNOScript API Guide</i> .
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routers and router components. Each router platform (M5 and M10 routers, M20 router, M40 router, M40e router, M160 router, and T640 routing node) has its own hardware guide.
<i>PIC Guide</i>	Describes the router Physical Interface Cards (PICs). Each router platform has its own PIC guide.

Documentation Feedback

We are always interested in hearing from our customers. Please let us know what you like and do not like about the Juniper Networks documentation, and let us know of any suggestions you have for improving the documentation. Also, let us know if you find any mistakes in the documentation. Send your feedback to tech-doc@juniper.net.

How to Request Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-2121 (from outside the United States).

Part 1

Overview

- Product Architecture on page 3
- JUNOS Software Overview on page 9
- Complete Configuration Mode Commands and Statements on page 33

Chapter 1

Product Architecture

The JUNOS Internet software provides IP routing protocol software—as well as software for interface, network, and chassis management—specifically designed for the large production networks typically supported by Internet service providers (ISPs). The JUNOS Internet software runs on all Juniper Networks routers. For more detailed information about hardware features, see the hardware installation guide for your router.

This chapter provides an overview of the router hardware and then discusses the relationships between the hardware and the software:

- Hardware Overview on page 3
- Product Architecture on page 4

Hardware Overview

The JUNOS Internet Software runs on two types of Juniper Networks routers: M- and T-series routers. The routers consist of the following major hardware components:

- Sheet metal of the chassis.
- Power supplies (AC or DC).
- Impeller trays.
- Fan assemblies.
- Routing Engine.
- System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), Switch Interface Board (SIB), or Forwarding Engine Board (FEB).
- Flexible PIC Concentrators (FPCs), each populated by up to four Physical Interface Cards (PICs) for various interface types, including SDH/SONET OC-192, OC-48, OC-12, and OC-3, ATM OC-12 and OC-3, DS3 (T3), E3, DS1 (T1), E1, Gigabit Ethernet, Fast Ethernet, and Channelized OC-12. Some PICs do not require an FPC.

Product Architecture

The router is composed of two components (see Figure 1):

- **Packet Forwarding Engine**—Forwards packets through the router. The Packet Forwarding Engine is a high-performance switch that is capable of forwarding 40 million packets of any size per second.

The Packet Forwarding engine uses ASICs to perform Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding. On M-series routers, the Packet Forwarding Engine includes the router (on the midplane, except on the M40 router, where it is on the backplane), Flexible PIC Concentrators (FPCs), Physical Interface Cards (PICs), and other components, unique to each router, that handle forwarding decisions.

The T-series routers feature multiple Packet Forwarding Engines, up to a maximum of 16 for the T640 Internet Routing Node and 8 for the T320 Internet Router. Each FPC has one or two Packet Forwarding Engines, each with its own memory buffer. Each Packet Forwarding Engine maintains a high-speed link to the Routing Engine. For information about T-series routers, see the *T640 Internet Routing Node Hardware Guide* and *T320 Internet Router Hardware guide*.



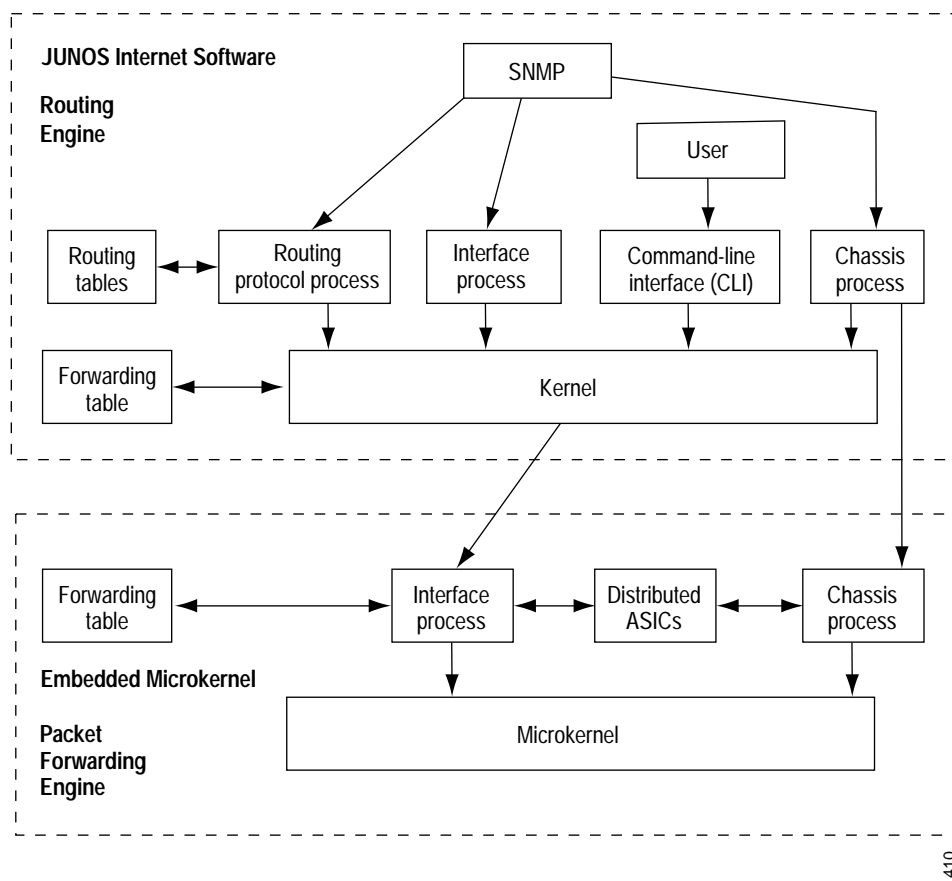
Note

T-series routers have multiple Packet Forwarding Engines, which are separate from the Routing Engines.

- **Routing Engine**—Performs routing updates and system management. The Routing Engine consists of routing-protocol software processes running inside a protected memory environment on a general-purpose computer platform. The Routing Engine has a direct 100-Mbps connection to the Packet Forwarding Engine.

Because this architecture separates control operations such as routing updates and system management from packet forwarding, the router can deliver superior performance and highly reliable Internet operation.

Figure 1: Product Architecture



Packet Forwarding Engine

The Packet Forwarding Engine forwards packets between input and output interfaces. The M-series and T-series routers use a different architecture for packet forwarding, and T-series routers can have multiple Packet Forwarding Engines.

Packet Flow through an M-Series Router

You can understand the function of the Packet Forwarding Engine by following the flow of a packet through the router—first into a PIC, then through the switching fabric, and finally out another PIC for transmission on a network link.

When a packet arrives on an input interface, a media-specific PIC performs all the media-specific actions, such as framing and checksum verification.

The PIC then passes a serial stream of bits into the FPC, which parses and appropriately deencapsulates the packet. For M-series routers, the FPC also breaks the packet into 64-byte memory blocks and passes each memory block to the Distributed Buffer Manager ASIC. The Distributed Buffer Manager ASIC or the Queuing and Memory Interface ASIC (on the T640 Internet routing node), and then writes the blocks into packet buffer memory, which is distributed evenly across all the FPCs installed in the router.

In parallel with the buffering, the Distributed Buffer Manager ASIC extracts the information from the packet needed for route lookup and passes that information to the Internet Processor ASIC or Internet Processor II ASIC, which performs a lookup in its full forwarding table and finds the outgoing interface and the specific next-hop. The forwarding table can forward all unicast packets that do not have options and multicast packets that have been previously cached. Unicast packets with options and noncached multicast packets are sent to the Routing Engine for resolution.

After the Internet Processor ASIC has determined the next-hop, it passes the results of the lookup to the second Distributed Buffer Manager ASIC or Queuing and Memory Interface ASIC, which in turn passes the results to the outgoing interface. (Note that there can be multiple outgoing interfaces if you are using multicast routing.)

At this stage, a pointer to the packet is queued, not the packet itself. Each output port has four queues, each of which has a configured share of the link bandwidth. Several factors can account for queuing order, including the value of the precedence bits, utilization of the input interface, destination address, and Random Early Detection (RED) and Weighted Random Early Detection (WRED) algorithms. If the outgoing interface decides to queue the packet to be sent, when the packet reaches the front of the queue and is ready for transmission, the memory blocks are read from packet buffer memory. Then the packet is reassembled and passed to the media-specific PIC for transmission on the line.

Packet Flow through a T-series Router

When a packet arrives on an input interface, the PIC performs media-specific operations such as framing and checksum verification and passes the packet to the FPC housing it. On the FPC, the Layer 2/Layer 3 Packet Processing ASIC parses the packet and divides it into data cells. The cells are sent to the Switch Interface ASIC, which extracts the notification and passes it to the T-series Internet Processor. The data cells are sent to the Queueing and Memory Interface ASIC, which manages data buffering on the FPC.

The Queueing and Memory ASIC sends the notification to the Switch Interface ASIC facing the switch fabric, which sends bandwidth requests to the destination FPC and issues read requests back to the Queueing and Memory ASIC to begin reading the data cells out of memory. The Switch Fabric ASIC on the destination FPC sends bandwidth grants to the originating Switch Fabric ASIC, which sends a cell to the destination FPC for each grant received.

On the destination FPC, the Switch Interface ASIC receives cells from the switch fabric. It extracts the route lookup key, places it in a notification, and forwards the notification to the T-series Internet Processor. The T-series Internet Processor performs the route lookup and forwards the notification to the Queueing and Memory ASIC, which passes it to the Switch Interface ASIC facing the network. The Switch Interface ASIC passes the cells to the Layer 2/Layer 3 Packet Processing ASIC, which reassembles them into packets, performs encapsulation, and sends the packets to the outgoing PIC. The PIC sends the packets out into the network.

Routing Engine

The Routing Engine handles all the routing protocol processes and other software processes that control the router's interfaces, a few of the chassis components, system management, and user access to the router. These routing and software processes run on top of a kernel that interacts with the Packet Forwarding Engine.

The Routing Engine has these features:

- Process routing protocol packets—All routing protocol packets from the network are directed to the Routing Engine, and therefore do not delay the Packet Forwarding Engine unnecessarily.
- Software modularity—By dividing software functions into separate processes, a failure of one process has little or no effect on the other software processes.
- In-depth Internet functionality—Each routing protocol is implemented with a complete set of Internet features and provides full flexibility for advertising, filtering, and modifying routes. Routing policies are set according to route parameters, such as prefix, prefix lengths, and BGP attributes.
- Scalability—The JUNOS routing tables are designed to hold all the routes in current and near-future networks. Additionally, the JUNOS software can efficiently support large numbers of interfaces and virtual circuits.
- Management interfaces—System management is possible with a command-line interface (CLI), a craft interface, and SNMP.
- Storage and change management—Configuration files, system images, and microcode can be held and maintained in one primary and two secondary storage systems, permitting local or remote upgrades.
- Monitoring efficiency and flexibility—Alarms can be generated and packets can be counted without adversely affecting packet forwarding performance.

The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the *forwarding table*, which is then copied into the Packet Forwarding Engine. The forwarding table in the Packet Forwarding Engine can be updated without interrupting the router's forwarding.



Chapter 2

JUNOS Software Overview

The JUNOS Internet software runs on the router's Routing Engine. It consists of software processes that support Internet routing protocols, control the router's interfaces and the router chassis itself, and allow router system management. All these processes run on top of a kernel that enables communication among all the processes and has a direct link to the Packet Forwarding Engine software. You use the JUNOS software to configure the routing protocols that should run on the router and to configure properties of the router's interfaces. Afterward, you use the JUNOS software to monitor the router and to troubleshoot protocol and network connectivity problems. For more information about monitoring the router and troubleshooting problems, see the *JUNOS Internet Software Operational Mode Command Reference*.

This chapter discusses the following topics:

- Routing Engine Software Components on page 9
- Software Installation Overview on page 15
- Tools for Accessing and Controlling the Software on page 15
- Software Configuration Overview on page 16
- Software Monitoring Tools on page 17
- Router Security on page 17
- Supported Software Standards on page 21

Routing Engine Software Components

The Routing Engine software consists of several software processes that control router functionality and a kernel that provides the communication among all the processes (see Figure 1 on page 5). This section describes the Routing Engine components:

- Routing Protocol Process on page 10
- Interface Process on page 14
- Chassis Process on page 14
- SNMP and MIB II Processes on page 14

- Management Process on page 15
- Routing Engine Kernel on page 15

Routing Protocol Process

The routing protocol process controls the routing protocols that run on the router. It starts all configured routing protocols and handles all routing messages. It maintains one or more routing tables, which consolidate the routing information learned from all routing protocols into common tables. From this routing information, the routing protocol process determines the active routes to network destinations and installs these routes into the Routing Engine's forwarding table. Finally, it implements routing policy, which allows you to control the routing information that is transferred between the routing protocols and the routing table. Using routing policy, you can filter routing information so that only some of it is transferred, and you also can set properties associated with the routes.

This section discusses the following topics:

- Routing Protocols (IPv4) on page 10
- Routing Protocols (IPv6) on page 12
- Routing and Forwarding Tables on page 12
- Routing Policy on page 13

Routing Protocols (IPv4)

The JUNOS software implements full IP routing functionality, providing support for IP Version 4 (IPv4). The routing protocols are fully interoperable with existing IP routing protocols, and they have been developed to provide the scale and control necessary for the Internet core.

The software provides the following routing and MPLS applications protocols:

- Unicast routing protocols
 - IS-IS—Intermediate System-to-Intermediate System is a link-state interior gateway protocol (IGP) for IP networks that uses the shortest-path-first (SPF) algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The JUNOS IS-IS software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
 - OSPF—Open Shortest Path First, Version 2, is an IGP that was developed for IP networks by the Internet Engineering Task Force (IETF). OSPF is a link-state protocol that makes routing decisions based on the SPF algorithm. The JUNOS OSPF software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
 - RIP—Routing Information Protocol, Version 2, is an IGP for IP networks based on the Bellman-Ford algorithm. RIP is a distance-vector protocol. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or to participate in the service provider's IGP discovery process.

- ICMP—Internet Control Message Protocol router discovery allows hosts to discover the addresses of operational routers on the subnet.
- BGP—Border Gateway Protocol, Version 4, is an exterior gateway protocol (EGP) that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with JUNOS routing policy, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.
- Multicast routing protocols
 - DVMRP—Distance Vector Multicast Routing Protocol is a dense-mode (flood-and-prune) multicast routing protocol.
 - PIM sparse mode and dense mode—Protocol-Independent Multicast is a multicast routing protocol. PIM sparse mode routes to multicast groups that might span wide-area and interdomain internets. PIM dense mode is a flood-and-prune protocol.
 - MSDP—Multicast Source Discovery Protocol allows multiple PIM sparse mode domains to be joined. A rendezvous point (RP) in a PIM sparse mode domain has a peer relationship with an RP in another domain, enabling it to discover multicast sources from other domains.
 - IGMP—Internet Group Management Protocol, Versions 1 and 2, is used to manage membership in multicast groups.
 - SAP/SDP—Session Announcement Protocol and Session Description Protocol handle conference session announcements.
- MPLS applications protocols
 - MPLS—Multiprotocol Label Switching, formerly known as tag switching, allows you to manually or dynamically configure label-switched paths (LSPs) through a network. It lets you direct traffic through particular paths rather than rely on the IGP's least-cost algorithm to choose a path.
 - RSVP—The Resource Reservation Protocol, Version 1, provides a mechanism for engineering network traffic patterns that is independent of the shortest path decided upon by a routing protocol. RSVP itself is not a routing protocol; it operates with current and future unicast and multicast routing protocols. The primary purpose of the JUNOS RSVP software is to support dynamic signaling for MPLS label-switched paths (LSPs).
 - LDP—The Label Distribution Protocol provides a mechanism for distributing labels in nontraffic-engineered applications. LDP allows routers to establish LSPs through a network by mapping network-layer routing information directly to data-link layer switched paths. LSPs created by LDP can also traverse LSPs created by RSVP.

Routing Protocols (IPv6)

The JUNOS software implements IP routing functionality, providing support for IP Version 6 (IPv6). The routing protocols have been developed to provide the scale and control necessary for the Internet core.

The software supports the following unicast routing protocols:

- IS-IS—Intermediate System-to-Intermediate System is a link-state interior gateway protocol (IGP) for IP networks that uses the shortest-path-first (SPF) algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The JUNOS software supports a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
- RIP—Routing Information Protocol version 2 is an IGP for IP networks based on the Bellman-Ford algorithm. RIP is a distance-vector protocol. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or to participate in the service provider's IGP discovery process.
- ICMP—Internet Control Message Protocol router discovery allows hosts to discover the addresses of operational routers on the subnet.
- BGP—Border Gateway Protocol version 4, is an exterior gateway protocol (EGP) that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with JUNOS routing policies, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.

Routing and Forwarding Tables

A major function of the JUNOS routing protocol process is to maintain the Routing Engine's routing tables and from these tables to determine the active routes to network destinations. The routing protocol process then installs these routes into the Routing Engine's forwarding table. The JUNOS kernel then copies this forwarding table to the Packet Forwarding Engine. Refer to Figure 1 on page 5 for an illustration of the interrelationships between the routing and forwarding tables.

The routing protocol process maintains multiple routing tables. By default, it maintains the following three routing tables. You can configure additional routing tables to suit your requirements.

- Unicast routing table—Stores routing information for all unicast routing protocols running on the router. IS-IS, OSPF, RIP, and BGP all store their routing information in this routing table. You can configure additional routes, such as static routes, to be included in this routing table. IS-IS, OSPF, RIP, and BGP use the routes in this routing table when advertising routing information to their neighbors.
- Multicast routing table (cache)—Stores routing information for all the running multicast protocols. DVMRP and PIM both store their routing information in this routing table, and you can configure additional routes to be included in this routing table.
- MPLS routing table—Stores MPLS path and label information.

With each routing table, the routing protocol process uses the collected routing information to determine active routes to network destinations.

For unicast routes, the routing protocol process determines active routes by choosing the most preferred route, which is the route with the lowest preference value. By default, the route's preference value is simply a function of how the routing protocol process learned about the route. You can modify the default preference value using routing policy and with software configuration parameters.

For multicast traffic, the routing protocol process determines active routes based on traffic flow and other parameters specified by the multicast routing protocol algorithms. The routing protocol process then installs one or more active routes to each network destination into the Routing Engine's forwarding table.

Routing Policy

By default, all routing protocols place their routes into the routing table. When advertising routes, the routing protocols by default advertise only a limited set of routes from the routing table. Specifically, each routing protocol exports only the active routes that were learned by that protocol. In addition, the IGPs (IS-IS, OSPF, and RIP) export the direct (interface) routes for the interfaces on which the protocol is explicitly configured.

You can control the routes that a protocol places into each table and the routes from that table that the protocol advertises. You do this by defining one or more routing policies and then applying them to the specific routing protocol.

Routing policies applied when the routing protocol places routes into the routing table are referred to as *import policies* because the routes are being imported into the routing table. Policies applied when the routing protocol is advertising routes that are in the routing table are referred to as *export policies* because the routes are being exported from the routing table. In other words, the terms *import* and *export* are used with respect to the routing table.

Routing policy allows you to control (filter) which routes a routing protocol imports into the routing table and which routes a routing protocol exports from the routing table. Routing policy also allows you to set the information associated with a route as it is being imported into or exported from the routing table. Filtering imported routes allows you to control the routes used to determine active routes. Filtering routes being exported from the routing table allows you to control the routes that a protocol advertises to its neighbors.

You implement routing policy by defining policies. A policy specifies the conditions to use to match a route and the action to perform on the route when a match occurs. For example, when a routing table imports routing information from a routing protocol, a routing policy might modify the route's preference, mark the route with a color to identify it and allow it to be manipulated at a later time, or prevent the route from even being installed in a routing table. When exporting routes from a routing table into a routing protocol, a policy might assign metric values, modify the BGP community information, tag the route with additional information, or prevent the route from being exported altogether. You also can define policies for redistributing the routes learned from one protocol into another protocol.

VPNs

The JUNOS software supports several types of VPNs:

- **Layer 2 VPNs**—A Layer 2 VPN links a set of sites sharing common routing information, and whose connectivity is controlled by a collection of policies. A Layer 2 VPN is not aware of routes within a customer's network. It simply provides private links between a customer's sites over the service provider's existing public Internet backbone.
- **Layer 3 VPNs**—A Layer 3 VPN links a set of sites that share common routing information, and whose connectivity is controlled by a collection of policies. A Layer 3 VPN is aware of routes within a customer's network, requiring more configuration on the part of the service provider than a Layer 2 VPN. The sites that make up a Layer 3 VPN are connected over a service provider's existing public Internet backbone.
- **Inter-provider VPNs**—An inter-provider VPN supplies connectivity between two VPNs in separate autonomous systems (ASs). This functionality could be used by a VPN customer with connections to several various ISPs, or different connections to the same ISP in various geographic regions.
- **Carrier-of-Carrier VPNs**—Carrier-of-carrier VPNs allow a VPN service provider to supply VPN service to a customer who is also a service provider. The latter service provider supplies Internet or VPN service to an end customer.

Interface Process

The JUNOS interface process allows you to configure and control the physical interface devices and logical interfaces present in a router. You can configure various interface properties such as the interface location (that is, which slot the FPC is installed in and which location on the FPC the PIC is installed in), the interface encapsulation, and interface-specific properties. You can configure the interfaces that currently are present in the router, as well as interfaces that currently are not present but that you may be adding at a future time.

The JUNOS interface process communicates, through the JUNOS kernel, with the interface process in the Packet Forwarding Engine, thus enabling the JUNOS software to track the status and condition of the router's interfaces.

Chassis Process

The JUNOS chassis process allows you to configure and control the properties of the router, including conditions that trigger alarms and clock sources. The chassis process communicates directly with a chassis process in the JUNOS kernel.

SNMP and MIB II Processes

The JUNOS software supports the Simple Network Management Protocol (SNMP), which helps administrators monitor the state of a router. The software supports SNMP Version 1 and Version 2 (also known as Version 2c, or v2c). The JUNOS implementation of SNMP does not include any of the security features that were originally included in the IETF SNMP drafts but were later dropped because of the inability to standardize on a particular method. The SNMP software is controlled by the JUNOS SNMP and MIB II processes, which consist of an SNMP master agent and various subagents.

Management Process

Within the JUNOS software, a process-controlling process starts and monitors all the other software processes. It also starts the command-line interface (CLI), which is the primary tool you use to control and monitor the JUNOS Internet software. This management process starts all the software processes and the CLI when the router boots. If a software process terminates, the management process attempts to restart it.

Routing Engine Kernel

The Routing Engine kernel provides the underlying infrastructure for all JUNOS software processes. In addition, it provides the link between the routing tables and the Routing Engine's forwarding table. It is also responsible for all communication with the Packet Forwarding Engine, which includes keeping the Packet Forwarding Engine's copy of the forwarding table synchronized with the master copy in the Routing Engine.

Software Installation Overview

The JUNOS Internet software is preinstalled on the router. Once the router is powered on, it is ready to be configured. The primary copy of the software is installed on a nonrotating flash disk. Two backup copies are included, one on the router's rotating hard disk and a second on the removable media (either an LS-120 floppy disk [a 120-MB disk] or a PCMCIA card) that is shipped with the router.

When the router boots, it first attempts to start the software image from the removable media if one is installed in the router. If this fails, the router next tries the flash disk, then finally the hard disk. Normally, you want the router to boot from the flash disk.

To upgrade the software, you copy a set of software images over the network to the router's flash disk using SCP or another similar utility. The JUNOS software set consists of three images, one for the software processes, a second for the kernel, and the third for the Packet Forwarding Engine. You normally upgrade all images simultaneously.

Tools for Accessing and Controlling the Software

The primary means of accessing and controlling the JUNOS software is the CLI.

The router provides three ports on the craft interface for connecting external management devices to the Routing Engine and the JUNOS Internet software:

- Console port—Connects a system console using an RS-232 serial cable.
- Auxiliary port—Connects a laptop or modem using an RS-232 serial cable.
- Ethernet management port—Connects the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management of the router. The Ethernet port is 10/100 Mbps autosensing and requires an RJ-45 connector.

The CLI is the interface to the JUNOS software that you use whenever you access the router from the console or through a remote network connection. The CLI provides commands that perform various tasks, including configuring the JUNOS software, and monitoring and troubleshooting the software, network connectivity, and the router hardware.

The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI provides command help and command completion; it also provides Emacs-style keyboard sequences that allow you to move around on a command line and scroll through a buffer that contains recently executed commands.

Software Configuration Overview

To configure the JUNOS software, you specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as some system hardware properties. After you have created a candidate configuration, you commit the configuration to be evaluated and activated by the JUNOS software.

This section discusses the following topics:

- Methods of Configuring the Software on page 16
- Configuring the Software on page 16
- Activating a Configuration on page 17

Methods of Configuring the Software

There are two basic ways to configure the JUNOS software:

- You can create the configuration for the router interactively, working in the CLI on the router.
- You can load an ASCII file containing a router configuration that you created earlier, either on this system or on another system. You can then activate and run the configuration file as is or you can edit it using the CLI and then activate it.

Configuring the Software

When you initially boot a router, the system prompts you for the minimal information needed to configure the router, including the router's name, domain name, and the Internet address of at least one interface on the router. After the router finishes this initial boot, you log in as the user "root" (with no password) and configure a password for the user "root."

After completing this initial minimal configuration, you can configure software properties. If you configure the software interactively using the CLI, you enter software configuration statements to create a candidate configuration that contains a hierarchy of statements. At any hierarchy level, you generally can enter statements in any order. While you are configuring the software, you can display all or portions of the candidate configuration, and you can insert or delete statements. Any changes you make affect only the candidate configuration, not the active configuration that is running on the router.

The configuration hierarchy logically groups related functions, which results in configuration statements that have a regular, consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy.

At each level of the hierarchy, you can display a list of the statements available at that level, along with short descriptions of the statements' functions. To have the CLI complete the statement name if it is unambiguous or to provide a list of possible completions, you can type a partial statement name followed by a space or tab.

More than one user can edit a router's configuration simultaneously. All changes made by all users are visible to everyone editing the configuration.

Activating a Configuration

To have a candidate configuration take effect, you commit the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

The CLI always maintains a copy of previously committed versions of the software configuration. If you need to return to a previous configuration, you can do this from within the CLI.

Software Monitoring Tools

The primary method of monitoring and troubleshooting the software, routing protocols, network connectivity, and the router hardware is to enter commands from the CLI. The CLI enables you to display information in the routing tables and routing protocol-specific data, and to check network connectivity using ping and traceroute commands.

The JUNOS software includes SNMP software, which allows you to manage routers. The SNMP software consists of an SNMP master agent and a MIB II agent, and supports MIB II SNMP version 1 traps and version 2 notifications, SNMP version 1 Get and GetNext requests, and version 2 GetBulk requests.

The software also supports tracing and logging operations so that you can track events that occur in the router—both normal router operations and error conditions—and track the packets that are generated by or pass through the router. Logging operations use a syslog-like mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging into or out of the router. Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions.

Router Security

Router security consists of three major elements: physical security of the router, operating system security, and security that can be effected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console. The inherent security of the JUNOS operating system also plays an important role in router security. The JUNOS software is extremely stable and robust. The JUNOS software also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

In designing your router configuration, you can increase router security by *hardening* the configuration, using the JUNOS features to apply sound security policies. In this way, virtually any router configuration should be capable of secure operation. Likewise, misconfiguring the JUNOS software can increase router vulnerability.

This section discusses some JUNOS software features available to improve router security:

- JUNOS Default Settings on page 18
- Router Access on page 19
- User Authentication on page 19
- Routing Protocol Security Features on page 20
- Firewall Filters on page 20
- Auditing for Security on page 20

JUNOS Default Settings

Immediately after installation and configuration of a root account password, the JUNOS software presents a hardened target by virtue of its default software settings. The following are some common router security weaknesses that the JUNOS software addresses in the default software settings:

- The JUNOS software does not forward directed broadcast messages. Directed broadcast services send ping requests from a spoofed source address to a broadcast address and can be used to attack other Internet users. For example, if broadcast ping messages were allowed on the 200.0.0.0/24 network, a single ping request could result in up to 254 responses, all aimed at the supposed source of the ping. The result would be that the source actually becomes the victim of a denial of service (DoS) attack.
- Only console access to the router is enabled by default. Remote management access to the router and all management access protocols, including telnet, ftp, and ssh, are disabled by default.
- The JUNOS software does not support the Simple Network Management Protocol (SNMP) set capability for editing configuration data. While the software does support the SNMP set capability for monitoring and troubleshooting the network, this support exposes no known security issues. (You can configure the software to disable this SNMP set capability.)
- The JUNOS software ignores martian addresses that contain the following prefixes: 0.0.0.0/8, 127.0.0.0/8, 128.0.0.0/16, 191.255.0.0/16, 192.0.0.0/24, 223.255.55.0/24, and 240.0.0.0/4. Martian addresses are reserved host or network addresses about which all routing information should be ignored.

Router Access

When you first install the JUNOS software, all remote access to the router is disabled, thereby ensuring that remote access is possible only if deliberately enabled by an authorized user. You can establish remote communication with a router in one of the following ways:

- **Out-of-band management**—Allows connection to the router through an interface dedicated to router management. Juniper Networks Routers support out-of-band management with a dedicated management Ethernet interface (fxp0), as well as EIA-232 console and auxiliary ports. The management Ethernet interface connects directly to the Routing Engine. No transit traffic is allowed through this interface, providing complete separation of customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the router.
- **Inband management**—Allows connection to the routers using the same interfaces through which customer traffic flows. While this approach is simple and requires no dedicated management resources, it has some disadvantages:
 - Management flows and transit traffic flows are mixed together. Any attack traffic that is mixed with the normal traffic can affect the communication with the router.
 - The links between the router might not be totally trustworthy, leading to the possibility of wiretapping and replay attacks.

For management access to the router, the standard ways to communicate with the router from a remote console are with telnet and the secure shell (ssh). ssh provides secure encrypted communications and is therefore useful for inband router management. Telnet provides unencrypted, and therefore less secure, access to the router.

User Authentication

On a route, you can create local user login accounts to control who can log in to the router and the access privileges they have. A password, either an ssh key or an MD5 password, is associated with each login account. To define access privileges, you create login classes into which you group users with similar jobs or job functions. You use these classes to explicitly define what commands their users are and are not allowed to issue while logged in to the router.

The management of multiple routers by many different personnel can create a user account management problem. One solution is to use a central authentication service to simplify account management, creating and deleting user accounts only on a single, central server. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks (attacks in which someone uses a captured password to pose as a router administrator).

The JUNOS software supports two protocols for central authentication of users on multiple routers—Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+). RADIUS is a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS.

Routing Protocol Security Features

The main task of a router is to forward user traffic toward its intended destination based on the information in the router's routing and forwarding tables. You can configure routing policies that define the flows of routing information through the network, controlling which routes the routing protocols place in the routing tables and which routes they advertise from the tables. You can also use routing policies to change specific route characteristics, effect changes to the default Border Gateway Protocol (BGP) route flap-damping values, perform per-packet load balancing, and enable class of service (CoS).

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn could degrade the functionality of the router. To prevent such attacks, you must ensure that routers form routing protocol peering or neighboring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The JUNOS BGP, OSPF, IS-IS, RIP, and RSVP protocols support HMAC-MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

The JUNOS software supports the Internet Protocol Security (IPSec) security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. The JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

Firewall Filters

Firewall filters allow you to control packets transiting the router to a network destination and packets destined for and sent by the router. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and to the Routing Engine. Firewall filters provide a means of protecting your router from excessive traffic. Firewall filters that control local packets can also protect your router from external aggressions, such as DoS attacks.

To protect the Routing Engine, you can configure a firewall filter only on the router's loopback interface. Adding or modifying filters for each interface on the router is not necessary. You can design firewall filters to protect against ICMP and TCP connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine.

Auditing for Security

The JUNOS software logs significant events that occur on the router and within the network. Although the logging of events and actions does not increase router security, you can use the system logs to monitor the effectiveness of your security policies and router configurations. You can also use the logs when reacting to a continued and deliberate attack as a means of identifying the source address, router, or port of the attacker's traffic. You can configure the logging of different levels of events, from only critical events to all events, including informational events. You can then inspect the contents of the system log files either in real time or at a later time.

Debugging and troubleshooting is much easier when the timestamps in the system log files of all routers are synchronized, because events that span the network might be correlated with synchronous entries in multiple logs. The JUNOS software supports the Network Time Protocol (NTP), which you can enable on the router to synchronize the system clocks of routers and other networking equipment. By default, NTP operates in an unauthenticated mode. You can configure various types of authentication, including an HMAC-MD5 scheme.

Supported Software Standards

This section lists the standards supported by the JUNOS software:

- Supported Internet RFCs and Drafts on page 21
- Supported ISO Standards on page 31
- Supported SDH and SONET Standards on page 31
- Other Supported Standards on page 32

To access Internet RFCs and drafts, go to the IETF web site: <http://www.ietf.org>.

Supported Internet RFCs and Drafts

This section lists the supported Internet RFCs and drafts.

ATM

- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed Protocol Data Units only)
- RFC 2225, *Classical IP and ARP over ATM* (responses only)
- RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed Protocol Data Units and ethernet bridged protocol data units only)

BGP

- RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1966, *BGP Route Reflection—An Alternative to Full-Mesh IGBP*
- RFC 1997, *BGP Communities Attribute*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
- RFC 2439, *BGP Route Flap Damping*

- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 3065, *Autonomous System Confederations for BGP*
- RFC 3107, *Carrying Label Information in BGP-4*
- *BGP/MPLS VPNs*, Internet Draft draft-ietf-ppvpn-rfc2547bis-00.txt
- *Capabilities Negotiation with BGP4*, Internet Draft draft-ietf-idr-cap-neg-01
- *BGP4+ Peering Using IPv6 Link-local Address*, Internet Draft draft-kato-bgp-ipv6-link-local-00.txt

CHAP

- RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

Frame Relay

- RFC 1490, *Multiprotocol Interconnect over Frame Relay*

GMPLS

- *Generalized MPLS - Signaling Functional Description*, Internet draft, draft-ietf-mppls-generalized-signaling-08.txt
 - generalized label request (only bandwidth encoding)
 - generalized label (only suggested label)
 - bidirectional LSPs (only upstream label)
 - control channel separation
- *Generalized MPLS Signaling - RSVP-TE Extensions*, Internet draft, draft-ietf-mppls-generalized-rsvp-te-07.txt
 - generalized label request object
 - generalized label object (only suggested labeled type)
 - bidirectional LSPs (only upstream label)
 - control channel separation (only IF-ID Hop object and IF-ID ErrSpec object)
 - new addressing for Path and PathTear messages.
- *GMPLS Extensions for SONET and SDH Control*, Internet draft-ietf-ccamp-gmpls-sonet-sdh-02.txt (only SUKLM labels and SONET traffic parameters)
- *LSP Hierarchy with Generalized MPLS TE*, Internet draft, draft-ietf-mppls-lsp-hierarchy-05.txt (only processing of IF-ID HOP object for RSVP-TE)

GRE and IP-IP Encapsulation

- RFC 1701, *Generic Routing Encapsulation (GRE)*
- RFC 1702, *Generic Routing Encapsulation over IPv4 Networks*
- RFC 2003, *IP Encapsulation within IP*

IP Multicast

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*
- RFC 2547, *BGP/MPLS VPNs*
- *Anycast RP Mechanism using PIM and MSDP*, Internet Draft draft-ietf-mboned-anycast-rp-05.txt
- *Bootstrap Router (BSR) Mechanism for PIM Sparse Mode*, Internet draft draft-ietf-pim-sm-bsr-02.txt
- *Distance Vector Multicast Routing Protocol*, Internet Draft draft-ietf-idmr-dvmrp-v3-07.txt
- *Internet Group Management Protocol, Version 3*, Internet Draft draft-ietf-idmr-igmp-v3-07.txt (only SAP, Version 0 and 1)
- *Multicast in MPLS/BGP VPNs*, Internet Draft draft-rosen-vpn-mcast-00.txt
- *Multicast Source Discovery Protocol (MSDP)*, Internet Draft draft-ietf-msdp-spec-01.txt
- *Protocol Independent Multicast-Version 2 Dense Mode Specification*, Internet Draft draft-ietf-pim-v2-dm-03.txt
- *SAP: Session Announcement Protocol*, Internet Draft draft-ietf-mmusic-sap-00.txt
- *Source-Specific Multicast for IP*, Internet Draft draft-holbrook-ssm-arch-02.txt

IPSec and IKE

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header (except for ES PIC)*
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulation Security Payload*
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *Internet Key Exchange*
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2412, *The OAKLEY Key Determination Protocol*

IPv6

- ISO/IEC 10589, *Information technology, Telecommunications and information exchange between systems, Intermediate system to intermediate system intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*
- RFC 1215, *A Convention for Defining Traps for Use with SNMP*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1965, *Autonomous System Confederations for BGP*
- RFC 1966, *BGP Route Reflection: An Alternative to Full-Mesh IBGP*
- RFC 1997, *BGP Communities Attribute*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- RFC 2283, *Multiprotocol Extensions for BGP-4*

- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
- RFC 2472, *IP Version 6 over PPP*
- RFC 2578, *Structure of Management Information Version 2 (SMIPv2)*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*
- *BGP Extended Communities Attribute*, Internet Draft draft-ramachandra-bgp-ext-communities-09.txt
- *Capabilities Negotiation with BGP4*, Internet Draft draft-ietf-idr-cap-neg-01.txt
- *Connecting IPv6 Islands across IPv4 Clouds with BGP*, draft-ietf-ngtrans-bgp-tunnel-04.txt (only MP-BGP over IPv4 Approach)
- *Routing IPv6 with IS-IS*, Internet Draft draft-ietf-isis-ipv6-02.txt

IS-IS

- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*
- RFC 2973, *IS-IS Mesh Groups*
- *IS-IS Extensions for Traffic Engineering*, Internet Draft draft-ietf-isis-traffic-02.txt
- *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*, Internet draft draft-ietf-isis-3way-03.txt

LDP

- *Label Distribution Protocol (LDP)—Version 1 Functional Specification*, (draft-ietf-mpls-ldp-06.txt)

MIBs

- IEEE, 802.3ad, *Aggregation of Multiple Link Segments* (only the objects dot3adAggMACAddress, dot3adAggAggregateOrIndividual, dot3adAggPortListPorts, and dot3adTablesLastChanged)
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (only isisSystem, isisMANAreaAddr, isisAreaAddr, isisSysProtSupp, isisSummAddr, isisCirc, isisCircLevel, isisPacketCount, isisISAdj, isisISAdjAreaAddr, isisAdjIPAddr, isisISAdjProtSupp, isisRa, and isisIPRA)
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. (except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096))
- RFC 1215, *Convention for Defining Traps for Use with the SNMP* (only MIB II SNMP version 1 traps and version 2 notifications)
- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIPv2*
- RFC 1850, *OSPF Version 2 Management Information Base* (except for the ospfOriginateNewLsas and ospfRxNewLsas objects, the Host Table, and the traps ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow)
- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIPv2*
- RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIPv2*
- RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIPv2*
- RFC 2096, *IP Forwarding Table MIB*
- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIPv2*
- RFC 2287, *Definitions of System-Level Managed Objects for Applications* (only sysApplInstallPkgTable, sysApplInstallElmtTable, sysApplElmtRunTable, and sysApplMapTable)
- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except IPv6 or ICMPv6 statistics)

- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types* (except for dsx1FarEndConfigTable, dsx1FarEndCurrentTable, dsx1FarEndIntervalTable, dsx1FarEndTotalTable, and dsx1FracTable)
- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type* (except dsx3FarEndConfigTable, dsx3FarEndCurrentTable, dsx3FarEndIntervalTable, dsx3FarEndTotalTable, and dsx3FracTable)
- RFC 2515, *Definitions of Managed Objects for ATM Management* (except atmVpCrossConnectTable, atmVcCrossConnectTable, and aal5VccTable)
- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type*
- RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)
- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)
- RFC 2573, *SNMP Applications*
- RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* (read-only access)
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol* (except row-creation, set operation and the object vrrpStatsPacketLengthErrors)
- RFC 2790, *Host Resources MIB* (only the objects of the hrSystem and hrSWInstalled groups)
- RFC 2819, *Remote Network Monitoring Management Information Base* (the etherStatsTable for Ethernet interfaces only and the objects alarmTable, eventTable, and logTable)
- RFC 2863, *The Interfaces Group MIB*
- RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations* (only the objects pingCtlTable, pingResultsTable, pingProbeHistoryTable, pingMaxConcurrentRequests, traceRouteCtlTable, traceRouteResultsTable, traceRouteProbeHistoryTable, and traceRouteHopsTable)
- RFC 2932, *IPv4 Multicast Routing MIB*
- *IANAiftype Textual Convention MIB*, Internet Assigned Numbers Authority (referenced by RFC 2233, available at <ftp://ftp.isi.edu/mib/ianaiftype.mib>)

- *Internet Group Management Protocol (IGMP) MIB*, Internet draft draft-ietf-idmr-igmp-mib-13.txt
- *Management Information Base for IS-IS*, Internet Draft draft-ietf-isis-wg-mib-07.txt (only isisISAdjTable, isisISAdjAreaAddrTable, isisISAdjIPAddrTable, and isisISAdjProtSuppTable)
- *Protocol Independent Multicast (PIM) MIB*, Internet Draft draft-ietf-idmr-pim-mib-09.txt

MPLS

- RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2216, *Network Element Service Specification Template*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*
- RFC 3032, *MPLS Label Stack Encoding*
- *BGP/MPLS VPNs*, Internet Draft draft-ietf-ppvpn-rfc2547bis-00.txt
- *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt (except node protection in facility backup)
- *ICMP Extensions for Multiprotocol Label Switching*, Internet Draft draft-ietf-mpls-icmp-01.txt
- *MPLS-based Layer 2 VPNs*, Internet Draft draft-kompella-ppvpn-l2vpn-00.txt
- *MPLS Label Stack Encoding*, Internet Draft draft-ietf-mpls-label-encaps-07.txt
- *Transport of Layer 2 Frames Over MPLS*, Internet Draft draft-martini-l2circuit-trans-mpls-07.txt

OSPF

- RFC 1587, *The OSPF NSSA Option*
- RFC 2328, *OSPF Version 2*
- *Traffic Engineering Extensions to OSPF*, Internet Draft draft-katz-yeung-ospf-traffic-01.txt

PPP

- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*
- RFC 2615, *PPP over SONET/SDH*

RIP

- RFC 1058, *Routing Information Protocol*
- RFC 2453, *RIP Version 2*

RSVP

- RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1, Functional Specification*
- RFC 2209, *Resource ReSerVation Protocol (RSVP), Version 1, Message Processing Rules*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2216, *Network Element Service Specification Template*
- RFC 2747, *RSVP Cryptographic Authentication*
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

SSL

- RFC 1319, *The MD2 Message-Digest Algorithm*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 2246, *The TLS Protocol Version 1.0*
- RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

TCP/IP v4

- RFC 768, *User Datagram Protocol*
- RFC 791, *Internet Protocol*
- RFC 792, *Internet Control Message Protocol*
- RFC 793, *Transmission Control Protocol*
- RFC 826, *Ethernet Address Resolution Protocol*
- RFC 854, *Telnet Protocol Specification*
- RFC 862, *Echo Protocol*
- RFC 863, *Discard Protocol*
- RFC 896, *Congestion Control in IP/TCP Internetworks*
- RFC 919, *Broadcasting Internet Datagrams*
- RFC 922, *Broadcasting Internet Datagrams in the Presence of Subnets*
- RFC 959, *File Transfer Protocol*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1042, *Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
- RFC 1157, *Simple Network Management Protocol (SNMP)*
- RFC 1166, *Internet Numbers*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation, and Analysis*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 2338, *Virtual Router Redundancy Protocol*

Supported ISO Standards

IS-IS

- ISO/IEC 10589, *Information technology, Telecommunications and information exchange between systems, Intermediate system to intermediate system intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*

Supported SDH and SONET Standards

- ANSI T1.105, *Synchronous Optical Network (SONET) Basic Description Including Multiplex Structures, Rates, and Formats*
- ANSI T1.105.02, *Synchronous Optical Network (SONET) Payload Mappings*
- ANSI T1.105.06, *SONET: Physical Layer Specifications*
- GR-253-CORE, *SONET Transport Systems: Common Generic Criteria*
- GR-499-CORE, *Transport System Generic Requirements (TSGR): Common Requirements*
- GR-1377-CORE, *SONET OC-192 Transport System Generic Criteria*
- ITU-T Recommendation G.691, *Optical interfaces for single channel SDH systems with optical amplifiers, and STM-64 systems*
- ITU-T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*
- ITU-T Recommendation G.783 (1994), *Characteristics of Synchronous Digital Hierarchy (SDH) equipment functional blocks*
- ITU-T Recommendation G.813 (1996), *Timing characteristics of SDH equipment slave clocks (SEC)*
- ITU-T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the Synchronous Digital Hierarchy (SDH)*
- ITU-T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate*
- ITU-T Recommendation G.831 (1993), *Management capabilities of transport networks based on Synchronous Digital Hierarchy (SDH)*
- ITU-T Recommendation G.957 (1995), *Optical interfaces for equipment and systems relating to the synchronous digital hierarchy*
- ITU-T Recommendation G.958 (1994), *Digital line systems based on the Synchronous Digital Hierarchy for use on optical fibre cables*
- ITU-T Recommendation I.432 (1993), *B-ISDN User-Network Interface Physical layer specification*

Other Supported Standards

ATM

- ITU-T Recommendation I.363, B-ISDN ATM adaptation layer sublayers: service-specific coordination function to provide the connection-oriented transport service (JUNOS software conforms only to the AAL5/IP over ATM portion of this standard)
- ITU-T Recommendation I.432.3, B-ISDN user-network interface Physical layer specifications: 51,840 kbits/s operation

Ethernet

- IEEE, 802.3ad, *Aggregation of Multiple Link Segments*
- IEEE, 802.3, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*

Frame Relay

- ANSI T1.617-1991, Annex D, Additional procedures for permanent virtual connections (PVCs) using unnumbered information frames
- ITU Q.933a, Annex A, Additional Procedures for Permanent Virtual Connections (PVC) status management (using Unnumbered Information frames)

T3

- ITU-T Recommendation G.703, Physical/electrical characteristics of hierarchical digital interfaces

Chapter 3

Complete Configuration Mode Commands and Statements

This chapter shows the complete configuration mode commands and the complete configuration statement hierarchy. Using these commands and statements is described in other chapters.

■ Complete Configuration Mode Commands on page 33

■ Complete Configuration Statement Hierarchy on page 34

For information about CLI operational mode commands, see the *JUNOS Internet Software Operational Mode Command Reference*. For information about IPv6 configuration statements, see the *JUNOS Internet Software Configuration Guide: IPv6*.

Complete Configuration Mode Commands

The following is the complete list of configuration mode commands, listing all possible commands in the hierarchy.

user@host# ?

Possible completions:

<[Enter]>	Execute this command
activate	Remove the inactive tag from a statement
annotate	Annotate the statement with a comment
commit	Commit current set of changes
copy	Copy a statement
deactivate	Add the inactive tag to a statement
delete	Delete a data element
edit	Edit a sub-element
exit	Exit from this level
help	Provide help information
insert	Insert a new ordered data element
load	Load configuration from an ASCII file
quit	Quit from this level
rename	Rename a statement
rollback	Roll back database to last committed version
run	Run an operational-mode command
save	Save configuration to an ASCII file
set	Set a parameter
show	Show a parameter
status	Display database user status
top	Exit to top level of configuration
up	Exit one level of configuration

Complete Configuration Statement Hierarchy

This section shows the complete configuration statement hierarchy, listing all possible configuration statements and showing their level in the configuration hierarchy. When you are configuring the JUNOS software, your current hierarchy level is shown in the banner on the line preceding the `user@host#` prompt.

This section is organized as follows:

- [edit access] Hierarchy Level on page 35
- [edit accounting-options] Hierarchy Level on page 35
- [edit chassis] Hierarchy Level on page 36
- [edit class-of-service] Hierarchy Level on page 37
- [edit firewall] Hierarchy Level on page 38
- [edit forwarding-options] Hierarchy Level on page 38
- [edit groups] Hierarchy Level on page 40
- [edit interfaces] Hierarchy Level on page 41
- [edit policy-options] Hierarchy Level on page 46
- [edit protocols] Hierarchy Level on page 46
- [edit routing-instances] Hierarchy Level on page 60
- [edit routing-options] Hierarchy Level on page 63
- [edit security] Hierarchy Level on page 66
- [edit snmp] Hierarchy Level on page 67
- [edit system] Hierarchy Level on page 69

[edit access] Hierarchy Level

```

profile profile-name {
  authentication-order [ authentication-methods ];
  client name chap-secret data;
  client name chap-secret data;
}
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
# End of [edit access] hierarchy level

```

[edit accounting-options] Hierarchy Level

```

accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  destination-class-profile profile-name {
    destination-class {
      destination-class-name;
    }
    file filename;
    interval minutes;
  }
  file filename {
    archive-sites {
      site-name;
    }
    file filename;
    size bytes;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}

```

```

routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
} # End of [edit accounting-options] hierarchy level

```

[edit chassis] Hierarchy Level

```

chassis {
    aggregated-devices {
        ethernet {
            device-count number;
        }
        sonet {
            device-count number;
        }
    }
    alarm {
        interface-type {
            alarm-name (red | yellow | ignore);
        }
    }
    fpcslot-number {
        pic pic-number {
            atm-cell-relay-accumulation;
            ce1 {
                e1 port-number {
                    channel-group group-number timeslots slot-number;
                }
            }
            ct3 {
                port port-number {
                    t1 link-number {
                        channel-group group-number timeslots slot-number;
                    }
                }
            }
        }
        framing (sdh | sonet);
        sparse-dlcis;
        no-concatenate;
        vtmapping (km | itu-t);
    }
}
(packet-scheduling | no-packet-scheduling);
(source-route | no-source-route);
redundancy {
    failover on-loss-of-keepalives;
    keepalive-timesecs;
    routing-engine slot-number (master | backup | disabled);
    sfm slot-number (always | preferred);
    ssb slot-number (always | preferred);
}
} # End of [edit chassis] hierarchy level

```


[edit class-of-service] Hierarchy Level

```

class-of-service {
  classifiers {
    (dscp | exp | ieee-802.1 | inet-precedence) classifier-name {
      import (classifier-name | default);
      forwarding-class class-name {
        loss-priority (low | high) code-points [ alias | bits ];
      }
    }
  }
  code-point-aliases {
    (dscp | exp | ieee-802.1 | inet-precedence) {
      alias-name bits;
    }
  }
  drop-profiles {
    profile-name {
      fill-level percentage drop-probability percentage;
      interpolate {
        drop-probability value;
        fill-level value;
      }
    }
  }
  forwarding-classes {
    queue queue-number class-name priority (low | high);
  }
  forwarding-policy {
    next-hop-map map-name {
      forwarding-class class-name {
        next-hop [ next-hop-name ];
        lsp-next-hop [ lsp-regular-expression ];
      }
    }
    class class-name {
      classification-override {
        forwarding-class class-name;
      }
    }
  }
  interfaces
    interface-name {
      scheduler-map map-name;
      unit logical-unit-number {
        classifiers {
          (dscp | exp | ieee-802.1 | inet-precedence) (classifier-name | default);
        }
        forwarding-class class-name;
        rewrite-rules {
          (dscp | exp | ieee-802.1 | inet-precedence) (rewrite-name | default);
        }
      }
    }
  }
}

```

```

rewrite-rules {
  (dscp | exp | ieee-802.1 | inet-precedence) rewrite-name {
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority (low | high) code-point (alias | bits);
    }
  }
}
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
schedulers
  scheduler-name {
    buffer-size ( percent percentage | remainder);
    drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any) drop-profile profile-name;
    priority (low | high | strict);
    transmit-rate (rate | percent percentage | remainder) <exact>;
  }
} # End of [edit class-of-service] hierarchy level

```

[edit firewall] Hierarchy Level

```

firewall {
  family family-name {
    filter filter-name;
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
    }
  }
} # End of [edit firewall] hierarchy level

```

[edit forwarding-options] Hierarchy Level

```

forwarding-options {
  hash-key {
    family inet {
      layer-3;
      layer-4;
    }
    family mpls {
      label-1;
      label-2;
    }
  }
}

```

```

helpers {
  bootp {
    description description-of-service;
    interface interface-group {
      description description-of-interface;
      maximum-hop-count number;
      minimum-wait-time seconds;
      no-listen;
      server [ address ]
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    server [ address ];
  }
  domain {
    description description-of-service;
    server address;
    interface interface-name {
      description description-of-interface;
      no-listen;
      server address;
    }
  }
}
tftp {
  description description-of-service;
  server address;
  interface interface-name {
    description description-of-interface;
    no-listen;
    server address;
  }
}
traceoptions {
  file filename;
  files number;
  size bytes;
}
flag flag;
level level;
}
sampling {
  disable;
  input {
    family inet {
      max-packets-per-second number;
      rate number;
      run-length number;
    }
  }
}

```

```

output {
  cflowd host-name {
    aggregation {
      autonomous-system;
      destination-prefix;
      protocol-port;
      source-destination-prefix {
        caida-compliant;
      }
      source-prefix;
    }
    autonomous-system-type (origin | peer);
    (local-dump | no-local-dump);
    port portnumber;
    version format;
  }
  file {
    filename filename;
    files number;
    size bytes;
    (stamp | no-stamp);
    (world-readable | no-world-readable);
  }
  port-mirroring {
    interface interface-name;
    next-hop address;
  }
}
tftp {
  server address;
  interface int0 {
    no-listen;
    server address;
  }
}
traceoptions {
  file filename {
    files number;
    size bytes;
    (world-readable | no-world-readable);
  }
}
}
} # End of [edit forwarding-options] hierarchy level

```

[edit groups] Hierarchy Level

```

groups {
  group-name {
    configuration-data;
  }
} # End of [edit groups] hierarchy level

```

[edit interfaces] Hierarchy Level

```

interfaces {
  interface-name {
    disable;
    accounting-profile name;
    description text;
    aggregated-ether-options {
      (flow-control | no-flow-control);
      link-speed speed;
      (loopback | no-loopback);
      minimum-links number;
      source-address-filter {
        mac-address;
      }
      (source-filtering | no-source-filtering);
    }
    aggregated-sonet options {
      link-speed speed;
      minimum-links number;
    }
    atm-options {
      promiscuous-mode;
      vpi vpi-identifier maximum-vcs maximum-vcs;
      ilmi;
      e3-options {
        atm-encapsulation (direct | PLCP);
        buildout distance (ft | m);
        framing (g751 | g832);
        loopback (local | remote);
        (payload-scrambler | no-payload-scrambler);
      }
      t3-options {
        atm-encapsulation (direct | PLCP);
        buildout distance (ft | m);
        (cbit-parity | no-cbit-parity);
        loopback (local | remote);
        (payload-scrambler | no-payload-scrambler);
      }
    }
  }
  clocking clock-source;
  dce;
  e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (32 | 16);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots slot-number;
  }
}

```

```

e3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    compatibility-mode (digital-link | kentrox) <subrate value>;
    fcs (32 | 16);
    idle-cycle-flag value;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
encapsulation type;
fastether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    ingress-rate-limit rate;
    (loopback | no-loopback);
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
gigether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    (loopback | no-loopback);
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
hold-time up milliseconds down milliseconds;
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
mac mac-address;
mtu bytes;
multiservice-options {
    boot-command filename
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
no-keepalives;
no-traps;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}

```

```

receive-bucket {
    overflow (tag | discard);
    rate percentage;
    threshold number;
}
sonet-options {
    aggregate asx;
    aps {
        advertise-interval milliseconds;
        authentication-key key;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        working-circuit group-name;
    }
    bytes {
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (32 | 16);
    loopback (local | remote);
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
    rfc-2615;
    (z0-increment | no-z0-increment);
}
speed (10m | 100m);
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout (0-133 | 133-266 | 266-399 | 399-532 | 532-655);
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (sf | esf);
    idle-cycle-flags (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots slot-number;
}

```

```

t3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (32 | 16);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow (discard);
    rate percentage;
    threshold number;
}
vlan-tagging;
unit logical-unit-number {
    access-profile-name;
    accounting-profile name;
    allow_any_vci;
    bandwidth;
    description text;
    disable;
    dlc dlci-identifier;
    drop-timeout milliseconds;
    encapsulation type;
    fragment-threshold bytes;
    inverse-arp;
    minimum-links number;
    mrru bytes;
    multicast-dlci dlci-identifier;
    multicast-vci vpi-identifier.vci-identifier;
    multipoint;
    no-traps;
    oam-liveness {
        up-count cells;
        down-count cells;
    }
    oam-period (disable | seconds);
    point-to-point;
    shaping {
        (cbr rate | vbr peak rate sustained rate burst length);
        queue-length number;
    }
    short-sequence;
    tunnel {
        source source-address;
        destination destination-address;
        routing-instance {
            destination routing-instance-name;
        }
        ttl number;
    }
}

```



```

vci vpi-identifier.vci-identifier;
vlan-id number;
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | [input output]);
        }
    }
}
bundle ml-fpc/pic/port;
filter {
    input filter-name;
    output filter-name;
    group filter-group-number;
}
ipsec-sa sa-name;
mtu bytes;
multicasts-only;
no-redirects;
policer {
    input policer-template-name;
    output policer-template-name;
}
primary;
remote mac-address address;
rpf-check fail-filter filter-name;
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    destination destination-address;
    eui-64;
    broadcast address;
    multipoint-destination destination-address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination destination-address {
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period seconds;
        shaping {
            (cbr rate | vbr peak rate sustained rate burst length);
            queue-length number;
        }
    }
    vci vpi-identifier.vci-identifier;
}
preferred;
primary;
vrrp-group group-number {
    virtual-address [ addresses ];
    priority number;
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    (preempt | no-preempt);
    track {
        interface interface-name priority-cost cost;
    }
}
}
}
}
} # End of [edit interfaces] hierarchy level

```

[edit policy-options] Hierarchy Level

```

policy-options {
  as-path name regular-expression;
  community name members [ community-ids ];
  damping name {
    disable;
    half-life minutes;
    max-suppress minutes;
    reuse number;
    suppress number;
  }
  policy-statement policy-name {
    term term-name {
      from {
        family family-name;
        match-conditions;
        policy subroutine-policy-name;
        prefix-list name;
        route-filter destination-prefix match-type <actions>;
        source-address-filter destination-prefix match-type <actions>;
      }
      to {
        match-conditions;
        policy subroutine-policy-name;
      }
      then actions;
    }
  }
  prefix-list name {
    ip-addresses;
  }
} # End of [edit policy-options] hierarchy level

```

[edit protocols] Hierarchy Level

```

protocols {
  BGP    bgp {
    advertise-inactive;
    authentication-key key;
    cluster cluster-identifier;
    damping;
    description text-description;
    disable;
    export [policy-name];
    family inet (inet | inet6 | inet-vpn | l2-vpn) {
      (any | unicast | multicast) {
        prefix-limit {
          maximum number;
          teardown <percentage> <idle-timeout (forever | time-in-minutes)>;
        }
      }
      rib-group group-name;
    }
  }
}

```

```

labeled-unicast {
  prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | time-in-minutes)>;
  }
  resolve-vpn;
  rib-group group-name;
}
}
graceful-restart (
  disable;
  restart-time seconds;
  stale-routes-time seconds;
)
hold-time seconds;
import [policy-name];
keep (all | none);
local-address address;
local-as autonomous-system <private>;
local-interface interface-name;
local-preference local-preference;
log-updown;
metric-out (metric | minimum-igp <offset> | igp <offset>;
multihop <ttl-value>;
no-aggregator-id;
no-client-reflect;
out-delay seconds;
passive;
path-selection (cisco-non-deterministic | always-compare-med);
peer-as autonomous-system;
preference preference;
remove-private;
traceoptions {
  file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
  flag flag <flag-modifier> <disable>;
}
group group-name {
  advertise-inactive;
  allow [network/mask-length];
  as-override;
  authentication-key key;
  cluster cluster-identifier;
  damping;
  description text-description;
  export [policy-name];
  family inet (inet | inet6 | inet-vpn | I2-vpn) {
    (any | unicast | multicast) {
      prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | time-in-minutes)>;
      }
      rib-group group-name;
    }
  }
  labeled-unicast {
    prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | time-in-minutes)>;
    }
    resolve-vpn;
    rib-group group-name;
  }
}
}

```

```

    graceful-restart (
    disable;
    restart-time seconds;
    stale-routes-time seconds;
    )
    hold-time seconds;
    import [policy-name];
    ipsec-sa ipsec-sa;
    keep (all | none);
    local-address address;
    local-as autonomous-system <private>;
    local-preference local-preference;
    log-updown;
    metric-out (metric | minimum-igp <offset> | igp <offset>);
    multihop <ttl-value>;
    multipath;
    no-aggregator-id;
    no-client-reflect;
    out-delay seconds;
    passive;
    peer-as autonomous-system;
    preference preference;
    protocol protocol;
    remove-private;
    traceoptions {
        file name <replace> <size size> <files number> <no-stamp>
            <(world-readable | no-world-readable)>;
        flag flag <flag-modifier> <disable>;
    }
    type type;
    neighbor address {
        advertise-inactive;
        as-override;
        authentication-key key;
        cluster cluster-identifier;
        damping;
        description text-description;
        export [policy-name];
        family inet (inet | inet6 | inet-vpn | l2-vpn) {
            (any | unicast | multicast) {
                prefix-limit {
                    maximum number;
                    teardown <percentage> <idle-timeout (forever | time-in-minutes)>;
                }
            }
            rib-group group-name;
        }
    }
    graceful-restart (
    disable;
    restart-time seconds;
    stale-routes-time seconds;
    )
    hold-time seconds;
    import [policy-name];
    ipsec-sa ipsec-sa;

    keep (all | none);
    local-address address;
    local-as autonomous-system <private>;
    local-preference local-preference;
    log-updown;
    metric-out (metric | minimum-igp <offset> | igp <offset>);
    multihop <ttl-value>;

```

```

        multipath;
        no-aggregator-id;
        no-client-reflect;
        out-delay seconds;
        passive;
        peer-as autonomous-system;
        preference preference;
        remove-private;
        traceoptions {
            file name <replace> <size size> <files number> <no-stamp>
                <(world-readable | no-world-readable)>;
            flag flag <flag-modifier> <disable>;
        }
    }
} # End of [edit protocols bgp] hierarchy level

Connections
connections {
    interface-switch connection-name {
        interface interface-name.unit-number;
        interface interface-name.unit-number;
    }
    lsp-switch connection-name {
        transmit-lsp label-switched-path;
        receive-lsp label-switched-path;
    }
    remote-interface-switch connection-name {
        interface interface-name.unit-number;
        transmit-lsp label-switched-path;
        receive-lsp label-switched-path;
    }
} # End of [edit protocols connections] hierarchy level

DVMRP
dvmrp {
    disable;
    export [ policy-names ];
    import [ policy-names ];
    interface interface-name {
        disable;
        hello-interval seconds;
        hold-time seconds;
        metric metric;
        mode (forwarding | unicast-routing);
    }
    rib-group group-name;
    inet;
}
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
} # End of [edit protocols dvmrp] hierarchy level

```

```

IGMP  igmp {
      interface interface-name {
        disable;
        static {
          group;
          group group {
            source source;
          }
        }
        version version;
        query-interval seconds;
        query-last-member-interval seconds;
        query-response-interval seconds;
        robust-count number;
        traceoptions {
          file name <replace> <size size> <files number> <no-stamp>
            <(world-readable | no-world-readable)>;
          flag flag <flag-modifier> <disable>;
        }
      }
    } # End of [edit protocols igmp] hierarchy level

IS-IS isis {
      disable;
      authentication-key key;
      authentication-type authentication;
      checksum;
      export [ policy-name ];
      ignore-attached-bit;
      graceful-restart {
        disable;
      }
      label-switched-path name level level metric metric;
      level level-number {
        authentication-key key;
        authentication-type authentication;
        external-preference preference;
        no-csnp-authentication;
        no-hello-authentication;
        no-psnp-authentication;
        preference preference;
        wide-metrics-only;
      }
      lsp-lifetime seconds;
      multicast-topology;
      no-authentication-check;
      overload <timeout seconds>;
      reference-bandwidth reference-bandwidth;
      rib-group group name;
      spf-delay milliseconds;

      traceoptions {
        file name <replace> <size size> <files number> <no-stamp>;
        <(world-readable | no-world-readable)>;
        flag flag <flag-modifier> <disable>;
      }
      traffic-engineering {
        disable;
        shortcuts;
      }
    }

```

```

interface interface-name {
    authentication-key key;
    authentication-type authentication;
    checksum;
    disable;
    csnp-interval (seconds | disable);
    hello-authentication-key key;
    hello-authentication-type authentication;
    lsp-interval milliseconds;
    mesh-group (value | blocked);
    passive;
    level level-number {
        authentication-key key;
        authentication-type authentication;
        disable;
        hello-authentication-key key;
        hello-authentication-type authentication;
        hello-interval seconds;
        hold-time seconds;
        metric metric;
        passive;
        priority number ;
        te-metric metric;
    }
}
} # End of [edit protocols isis] hierarchy level

L2vpn    l2vpn {
    encapsulation-type <type>
    traceoptions {
        file filename <replace> <size size> <files number> <nostamp>;
        flag flag <flag-modifier> <disable>;
    }
    site site-name {
        site-identifier identifier;
        interface interface-name {
            site-offset offset;
        }
    }
} # End of [edit protocols l2vpn] hierarchy level

L2circuit    l2circuit {
    neighbor address {
        interface interface-name {
            virtual-circuit-id identifier;
        }
    }
    traceoptions {
        file file-name [replace] [size number] [files file-names] [nostamp];
        flag (connections | error | FEC | topology) [detail];
    }
} # End of [edit protocols l2circuit] hierarchy level

```

```

LDP    ldp {
        import policy-name;
        deaggregate | no-deaggregate;
        egress-policy policy-name;
        export policy-name;
        keepalive-interval seconds;
        keepalive-timeout seconds;
        preference preference;
        transport-address (interface | loopback);
        interface interface-name {
            disable;
            hello-interval seconds;
            hold-time seconds;
            deaggregate | no-deaggregate;
            transport-address (interface | loopback);
        }
        traceoptions {
            file filename <replace> <size size> <files number> <no-stamp>
              <(world-readable | no-world-readable)>;
            flag flag <flag-modifier> <disable>;
        }
        traffic-statistics {
            file filename <replace> <size size> <files number> <(world-readable | no-world-readable)>;
            interval interval;
        }
    } # End of [edit protocols ldp] hierarchy level

```

```

Link management    link-management {
                    te-link te-link-name {
                        local-address ipv4_address;
                        remote-address ipv4_address;
                        remote-id number;
                        interface interface-name {
                            remote-id number;
                            local-address ipv4_address;
                            remote-address ipv4_address;
                        }
                    }
                } # End of [edit protocols link-management] hierarchy level

```

```

MPLS    mpls {
        admin-groups {
            group-name group-value;
        }
        bandwidth bandwidth;
        class-of-service cos-value;
        disable;
        hop-limit number;
        log-updown {
            (syslog | no-syslog);
            (trap | no-trap);
        }
        no-cspf;
        no-decrement-ttl;
        no-propagate-ttl;
        no-record;
        optimize-aggressive;
        path path-name {
            address <strict | loose>;
        }
    }

```



```

preference preference;
priority setup-priority hold-priority;
record;
rvsp-error-hold-time seconds;
standby;
statistics {
    auto-bandwidth;
    file filename <size size> <files number> <no-stamp>;
    interval seconds;
}
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs);
label-switched-path lsp-path-name {
    disable;
    to address;
    from address;
    adaptive;
    admin-group {
        exclude [ group-names ];
        include [ group-names ];
    }
    autobandwidth {
        adjust-interval seconds;
        maximum-bandwidth bps;
        minimum-bandwidth bps;
        monitor-bandwidth;
    }
    bandwidth bps;
    class-of-service cos-value;
    fast-reroute {
        bandwidth bps;
        (exclude group-names | no-exclude);
        hop-limit number;
        (include group-names | no-include);
    }
    from address;
    hop-limit number;
    install {
        destination-prefix/prefix-length <active>;
    }
    ldp-tunneling;
    lsp-attributes {
        bidirectional;
        encoding-type encoding-type;
        gpipid gpipid;
        signal-type signal-type;
        switching-type switching-type;
    }
    (link-protection | no-link-protection);
    metric metric;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority hold-priority;
    (random | least-fill | most-fill);
    (record | no-record);
    retry-limit number;
    retry-timer seconds;

```

```

standby;
primary path-name {
  adaptive;
  admin-group {
    include [ group-names ];
    exclude [ group-names ];
  }
  bandwidth bps;
  class-of-service class-of-service;
  hop-limit number;
  no-cspf;
  no-decrement-ttl;
  optimize-timer seconds;
  preference preference;
  priority setup-priority hold-priority;
  (record | no-record);
  standby;
}
secondary path-name {
  adaptive;
  admin-group {
    include group-names;
    exclude group-names;
  }
  bandwidth bps;
  class-of-service class-of-service;
  hop-limit number;
  no-cspf;
  optimize-timer seconds;
  preference preference;
  priority setup-priority hold-priority;
  (record | no-record);
  standby;
}
to address;
}
interface (interface-name | all) {
  disable;
  admin-group {
    group-name;
  }
  label-map in-label {
    (next-hop (address | interface-name | address/interface-name)) | (reject | discard);
    (pop | swap <out-label>);
    class-of-service class-of-service;
    preference preference;
    type type;
  }
}
static-path inet {
  prefix {
    next-hop (address | interface-name | address/interface-name);
    push out-label;
    class-of-service class-of-service;
    preference preference;
  }
}
} # End of [edit protocols mpls] hierarchy level

```

MSDP	<pre> msdp { disable; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local address <i>address</i>; rib-group <i>group-name</i>; traceoptions { file <i>name</i> <replace> <size <i>size</i>> <files <i>number</i>> <no-stamp> <(world-readable no-world-readable)>; flag <i>flag</i> <flag-modifier> <disable>; } peer <i>address</i> { disable; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local-address <i>address</i>; traceoptions { file <i>name</i> <replace> <size <i>size</i>> <files <i>number</i>> <no-stamp> <(world-readable no-world-readable)>; flag <i>flag</i> <flag-modifier> <disable>; } } group <i>group-name</i> { disable; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local-address <i>address</i>; mode <(mesh-group standard)>; traceoptions { file <i>name</i> <replace> <size <i>size</i>> <files <i>number</i>> <no-stamp> <(world-readable no-world-readable)>; flag <i>flag</i> <flag-modifier> <disable>; } } peer <i>address</i>; { disable; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local-address <i>address</i>; traceoptions { file <i>name</i> <replace> <size <i>size</i>> <files <i>number</i>> <no-stamp> <(world-readable no-world-readable)>; flag <i>flag</i> <flag-modifier> <disable>; } } } } # End of [edit protocols msdp] hierarchy level </pre>	
Neighbor Discovery	<pre> router-advertisement { interface <i>interface-name</i> { current-hop-limit <i>number</i>; default-lifetime <i>seconds</i>; (managed-configuration no-managed-configuration); max-advertisement-interval <i>seconds</i>; min-advertisement-interval <i>seconds</i>; (other-stateful-configuration no-other-stateful-configuration); prefix <i>prefix</i> { (autonomous no-autonomous); (on-link no-on-link); preferred-lifetime <i>seconds</i>; valid-lifetime <i>seconds</i>; } } } </pre>	

```

    reachable-time milliseconds;
    retransmit-timer milliseconds;
    traceoptions {
        file name <replace> <size size> <files number> <no-stamp>
            <(world-readable | no-world-readable)>;
        flag flag <detail> <disable>;
    }
}
} # End of [edit protocols router-advertisement] hierarchy level

```

```

OSPF    ospf {
        disable;
        domain-id domain-id;
        export [ policy-name ];
        external-preference preference;
        graceful-restart {
            disable;
            helper-disable;
            notify-duration seconds;
            rest-duration seconds;=
        }
        overload {
            <timeout seconds>;
        }
        preference preference;
        reference-bandwidth reference-bandwidth;
        rib-group group-name;
        route-type-community (vendor | iana);
        traffic-engineering {
            no-topology;
            shortcuts;
        }
        traceoptions {
            file name <replace> <size size> <files number> <no-stamp>
                <(world-readable | no-world-readable)>;
            flag flag <flag-modifier> <disable>;
        }
        area area-id {
            area-range network/masklen <restrict>;
            authentication-type authentication;
            interface interface-name {
                disable;
                authentication-key key <key-id identifier>;
                dead-interval seconds;
                hello-interval seconds;
                interface-type type;
                metric metric;
                neighbor address <eligible>;
                passive;
                poll-interval seconds;
                priority number;
                retransmit-interval seconds;
                transit-delay seconds;
                transmit-interval seconds;
            }
        }
    }

```

```

label-switched-path name metric metric;
nssa {
    area-range network/masklen <restrict>;
    default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
    }
    (no-summaries | summaries);
}
stub <default-metric metric> <(no-summaries | summaries)>;
virtual-link neighbor-id router-id transit-area area-id {
    disable;
    authentication-key key <key-id identifier>;
    dead-interval seconds;
    hello-interval seconds;
    retransmit-interval seconds;
    transit-delay seconds;
}
}
} # End of [edit protocols ospf] hierarchy level

```

PIM

```

pim {
    disable;
    dense-groups {
        addresses;
    }
    import [ policy-names ];
    interface interface-name {
        disable;
        mode (dense | sparse | sparse-dense);
        priority number;
        version version;
    }
    rib-group group-name;
    rp {
        disable;
        address address;
        group-ranges {
            destination-mask;
        }
        hold-time seconds;
        priority number;
    }
    auto-rp (announce | discovery | mapping);
    bootstrap-priority number;
    bootstrap-import pim-import;
    bootstrap-export pim-export;
    static {
        address address {
            version version;
            group-ranges {
                destination-mask;
            }
            traceoptions {
                file name <replace> <size size> <files number> <no-stamp>
                <(world-readable | no-world-readable)>;
                flag flag <flag-modifier> <disable>;
            }
        }
    }
}
} # End of [edit protocols pim] hierarchy level

```

```

RIP    rip {
        authentication-key password;
        authentication-type type;
        (check-zero | no-check-zero);
        import [ policy-names ];
        message-size number;
        metric-in metric;
        receive receive-options;
        rib-group group-name;
        send send-options;
        traceoptions {
            file name <replace> <size size> <files number> <no-stamp>
              <(world-readable | no-world-readable)>;
            flag flag <flag-modifier> <disable>;
        }
        group group-name {
            export [ policy-names ];
            metric-out metric;
            preference preference;
            neighbor neighbor-name {
                authentication-key password;
                authentication-type type;
                (check-zero | no-check-zero);
                import [ policy-names ];
                message-size number;
                metric-in metric;
                receive receive-options;
                send send-options;
            }
        }
    } # End of [edit protocols rip] hierarchy level

```

```

RIPng  ripng {
        import [ policy-names ];
        metric-in metric;
        receive <none>;
        send <none>;
        traceoptions {
            file name <replace> <size size> <files number> <no-stamp>
              <(world-readable | no-world-readable)>;
            flag flag <flag-modifier> <disable>;
        }
        group group-name {
            export [ policy-names ];
            metric-out metric;
            preference number;
            neighbor interface-name {
                import [ policy-names ];
                metric-in metric;
                receive <none>;
                send <none>;
            }
        }
    } # End of [edit protocols ripng] hierarchy level

```

Router Advertisement

```

router-advertisement {
  interface interface-name {
    current-hop-limit number;
    default-lifetime seconds;
    (managed-configuration | no-managed-configuration);
    max-advertisement-interval seconds;
    min-advertisement-interval seconds;
    (other-stateful-configuration | no-other-stateful-configuration);
    prefix prefix {
      (autonomous | no-autonomous);
      (on-link | no-on-link);
      preferred-lifetime seconds;
      valid-lifetime seconds;
    }
    reachable-time milliseconds;
    retransmit-timer milliseconds;
    traceoptions {
      file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
      flag flag <detail> <disable>;
    }
  }
}

```

Router Discovery

```

router-discovery {
  disable;
  traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
      <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
  }
  interface interface-name {
    min-advertisement-interval seconds;
    max-advertisement-interval seconds;
    lifetime seconds;
  }
  address address {
    (advertise | ignore);
    (broadcast | multicast);
    (priority number | ineligible);
  }
} # End of [edit protocols router-discovery] hierarchy level

```

RSVP

```

rsvp {
  disable;
  keep-multiplier number;
  preemption (aggressive | disabled | normal);
  refresh-time seconds;
  traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
      <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
  }
}

```

```

interface interface-name {
    disable;
    (aggregate | no-aggregate);
    authentication-key key;
    bandwidth bps;
    hello-interval seconds;
    link-protection {
        bandwidth bandwidth;
        class-of-service class-of-service-value;
        disable;
    }
    subscription percentage;
}
} # End of [edit protocols rsvp] hierarchy level

SDP/SAP    sap {
    disable;
    listen <address> <port port>;
} # End of [edit protocols sap] hierarchy level

VRRP    traceoptions {
    file {
        filename filename;
        files number;
        size size;
        (world-readable | no-world-readable);
    }
    flag flag;
}

```

[edit routing-instances] Hierarchy Level

```

routing-instances {
    routing-instance-name {
        description text;
        interface interface-name;
        instance-type (forwarding | l2vpn | no-forwarding | vrf);
        route-distinguisher (as-number:number | ip-address:number);
        vrf-import [policy-name];
        vrf-export [policy-name];
        vrf-table-label;
        protocols {
            bgp {
                bgp-configuration;
            }
            isis {
                isis-configuration;
            }
            l2vpn {
                l2vpn-configuration;
            }
            ldp {
                ldp-configuration;
            }
            ospf {
                ospf-configuration;
            }
            pim {
                pim-configuration;
            }
        }
    }
}

```



```

rip {
    rip-configuration;
}
}
routing-options {
    aggregate {
        defaults {
            aggregate-options;
        }
        route destination-prefix {
            policy policy-name;
            aggregate-options;
        }
    }
}
auto-export {
    (disable | enable);
    family {
        inet {
            multicast {
                (disable | enable);
                rib-group rib-group;
            }
            unicast {
                (disable | enable);
                rib-group rib-group;
            }
        }
    }
}
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
}
autonomous-system autonomous-system <loops number>;
confederation confederation-autonomous-system members autonomous-system;
fate-sharing {
    group group-name;
    cost value;
    from address [to address];
}
forwarding-table {
    export [ policy-name ];
}
generate {
    defaults {
        generate-options;
    }
    route destination-prefix {
        policy policy-name;
        generate-options;
    }
}
instance-export [ policy-names ];
instance-import [ policy-names ];
interface-routes {
    rib-group group-name;
}
martians {
    destination-prefix match-type <allow>;
}

```

```

maximum-routes route-limit <log-only | threshold value>;
multicast {
    scope scope-name {
        interface interface-name;
        prefix destination-prefix;
    }
    ssm-groups {
        addresses;
    }
}
options {
    syslog (level level | upto level);
}
resolution {
    tracefilter [filter-policy];
    traceoptions {
        file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
        flag flag <flag-modifier> <disable>;
    }
}
rib routing-table-name {
    aggregate {
        defaults {
            aggregate-options;
        }
        route destination-prefix {
            policy policy-name;
            aggregate-options;
        }
    }
    generate {
        defaults {
            generate-options;
        }
        route destination-prefix {
            policy policy-name;
            generate-options;
        }
    }
}
martians {
    destination-prefix match-type <allow>;
}
static {
    defaults {
        static-options;
    }
    rib-group group-name;
    route destination-prefix {
        lsp-next-hop {
            metric metric;
            preference preference;
        }
        next-hop;
        qualified-next-hop address {
            metric metric;
            preference preference;
        }
        static-options;
    }
}
}

```

```

rib-groups {
    group-name {
        import-policy [policy-name];
        import-rib [ group-name ];
        export-rib [ group-name ];
    }
}
route-record;
router-id address;
static {
    defaults {
        static-options;
    }
    rib-group group-name;
    route destination-prefix {
        lsp-next-hop {
            metric metric;
            preference preference;
        }
        next-hop;
        qualified-next-hop address {
            metric metric;
            preference preference;
        }
        static-options;
    }
}
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
}
} # End of [edit routing-instances] hierarchy level

```

[edit routing-options] Hierarchy Level

```

routing-options {
    aggregate {
        defaults {
            aggregate-options;
        }
    }
    route destination-prefix {
        policy policy-name;
        aggregate-options;
    }
}

```

```

auto-export {
  (disable | enable);
  family {
    inet {
      multicast {
        (disable | enable);
        rib-group rib-group;
      }
      unicast {
        (disable | enable);
        rib-group rib-group;
      }
    }
  }
}

traceoptions {
  file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
  flag flag <flag-modifier> <disable>;
}

autonomous-system autonomous-system <loops number>;
confederation confederation-autonomous-system members autonomous-system;
fate-sharing {
  group group-name;
  cost value;
  from address [to address];
}

forwarding-table {
  export [ policy-name ];
  unicast-reverse-paths (active-paths | feasible-paths);
}

generate {
  defaults {
    generate-options;
  }
  route destination-prefix {
    policy policy-name;
    generate-options;
  }
}

graceful-restart {
  disable;
  path-selection-defer-time-limit time limit;
}

instance-export [ policy-names ];
instance-import [ policy-names ];
interface-routes {
  rib-group group-name;
}

martians {
  destination-prefix match-type <allow>;
}

maximum-routes route-limit <log-only | threshold value>;
multicast {
  scope scope-name {
    interface interface-name;
    prefix destination-prefix;
  }
  ssm-groups {
    address;
  }
}

```

```

options {
    syslog (level level | upto level);
}
resolution {
    tracefilter [filter-policy];
    traceoptions {
        file name <replace> <size size> <files number> <no-stamp>
            <(world-readable | no-world-readable)>;
        flag flag <flag-modifier> <disable>;
    }
}
rib routing-table {
    aggregate {
        defaults {
            aggregate-options;
        }
        rib-group group-name;
        route destination-prefix {
            policy policy-name;
            aggregate-options;
        }
    }
}
generate {
    defaults {
        generate-options;
    }
    route destination-prefix {
        policy policy-name;
        generate-options;
    }
}
martians {
    destination-prefix match-type <allow>;
}
static {
    defaults {
        static-options;
    }
    rib-group group-name;
    route destination-prefix {
        lsp-next-hop {
            metric metric;
            preference preference;
        }
        next-hop;
        qualified-next-hop address {
            metric metric;
            preference preference;
        }
        static-options;
    }
}
rib-groups {
    group-name {
        import-policy [ policy-name ];
        import-rib [ group-name ];
        export-rib [ group-name ];
    }
}

```

```

route record;
router-id address;
static {
    defaults {
        static-options;
    }
    rib-group group-name;
    route destination-prefix {
        lsp-next-hop {
            metric metric;
            preference preference;
        }
        next-hop;
        qualified-next-hop address {
            metric metric;
            preference preference;
        }
        static-options;
    }
}
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
} # End of [edit routing-options] hierarchy level

```

[edit security] Hierarchy Level

```

security
certificates local certificate-name;
ike {
    proposal ike-proposal-name {
        authentication-algorithm (md5 | sha1);
        authentication-method pre-shared-keys;
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
    }
    policy ike-peer-address {
        mode (aggressive | main);
        proposal [ike-proposal-names];
        pre-shared-key (ascii-text key | hexadecimal key);
    }
}
ipsec {
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol esp;
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposal [ipsec-proposal-names];
    }
}

```

```

security-association name {
  mode (tunnel | transport);
  manual {
    direction (inbound | outbound | bi-directional) {
      spi spi-value;
      protocol (esp | ah);
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
    }
  }
  dynamic {
    <security-association (32 | 64)>;
    ipsec-policy policy-name;
  }
  traceoptions {
    file <files number> <size size>;
    flag all;
    flag database;
    flag general;
    flag ike;
    flag parse;
    flag policy-manager;
    flag routing-socket;
    flag timer;
  }
}
} # End of [edit security] hierarchy level

```

[edit snmp] Hierarchy Level

```

snmp {
  access {
    context context-name {
      description description;
      group group-name {
        model usm;
        read-view view-name;
        security-level (none | authentication | privacy);
        write-view view-name;
      }
    }
  }
  group group-name {
    model usm;
    user [ user-name ];
  }
}

```

```

user [ user-name ] {
    authentication-password authentication-password;
    authentication-type (none | md5 | sha);
    privacy-password privacy-password;
    privacy-type (none | des);
    clients {
        address restrict;
    }
}
}
}
community community-name {
    authorization authorization;
    clients {
        address restrict;
    }
    view view-name;
}
contact contact;
description description;
interface [ interface-name ];
location location;
name name;
traceoptions {
    file size size files number;
    flag flag;
}
engine-id {
    local engine-id;
}
}
rmon {
    alarm index {
        description text-description;
        falling-event-index index;
        falling-threshold integer;
        interval seconds;
        rising-event-index index;
        rising-threshold integer;
        sample-type type;
        startup-alarm alarm;
        variable oid-variable;
    }
    event index {
        community community-name;
        description text-description;
        type type;
    }
}
trap-group group-name {
    categories category;
    destination-port <port-number>;
    targets {
        address;
    }
    version version;
}

```



```

trap-options {
    agent-address outgoing-interface;
    source-address address;
}
view view-name;
    oid object-identifier (include | exclude)
}
} # End of [edit snmp] hierarchy level

```

[edit system] Hierarchy Level

```

system {
    authentication-order [ authentication-methods ];
    backup-router address <destination destination-address>;
    compress-configuration-files;
    default-address-selection;
    dhcp-relay {
        no-listen;
        maximum-hop-count;
        minimum-wait-time seconds;
        server [ address ];
        interface interface-group {
            no-listen;
            maximum-hop-count;
            minimum-wait-time seconds;
            server [ address ];
        }
    }
    diag-port-authentication (encrypted-password "password" | plain-text-password);
    domain-name domain-name;
    domain-search [ domain-list ];
    host-name host-name;
    location {
        altitude feet;
        country-code code;
        hcoord horizontal-coordinate;
        lata service-area;
        latitude degrees;
        longitude degrees;
        npa-nxx number;
        postal-code postal-code;
        vcoord vertical-coordinate;
    }
    login {
        message text;
        class class-name {
            allow-commands "regular-expression";
            allow-configuration "regular-expression";
            deny-commands "regular-expression";
            deny-configuration "regular-expression";
            idle-timeout minutes;
            permissions [ permissions ];
        }
    }
}

```

```

user user-name {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}

mirror-flash-on-disk;
name-server {
    address;
}

no-redirects;
no-saved-core-context;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}

ports {
    auxiliary {
        type terminal-type;
    }
    console {
        type terminal-type;
    }
}

processes {
    inet-process (enable | disable) failover (alternate-media | other-routing-engine);
    interface-control (enable | disable) failover (alternate-media | other-routing-engine);
    mib-process (enable | disable) failover (alternate-media | other-routing-engine);
    ntp (enable | disable) failover (alternate-media | other-routing-engine);
    routing (enable | disable) failover (alternate-media | other-routing-engine);
    snmp (enable | disable) failover (alternate-media | other-routing-engine);
    watchdog (enable | disable) failover (alternate-media | other-routing-engine) timeout seconds;
}

radius-server server-address {
    port number;
    retry number;
    secret password;
    timeout seconds;
}

root-authentication {
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
}

```

```

services {
  finger {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  ftp {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  rlogin {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    <connection-limit limit>;
    <rate-limit limit>;
  }
  telnet {
    <connection-limit limit>;
    <rate-limit limit>;
  }
}
static-host-mapping {
  host-name {
    inet [ address ];
    sysid system-identifier;
    alias [ alias ];
  }
}
syslog {
  file filename {
    facility level;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
  host hostname {
    facility level;
    facility-override facility;
    log-prefix string;
  }
  user (username | *) {
    facility level;
  }
  console {
    facility level;
  }
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
}

```

```
tacplus-server server-address {  
    secret password;  
    single-connection;  
    timeout seconds;  
}  
time-zone time-zone;  
} # End of [edit system] hierarchy level
```

Part 2

Software Installation and Upgrade

- Installation Overview on page 75
- Configure the Software Initially on page 81
- Reinstall the Software on page 85
- Upgrade Software Packages on page 89
- Upgrade to Release 5.0 or Downgrade from Release 5.0 on page 95

Chapter 4

Installation Overview

Your router comes with JUNOS software installed on it. When you power on the router, all software starts automatically. You simply need to configure the software and the router will be ready to participate in the network.

The software is installed on the router's flash drive (a nonrotating drive) and hard drive (a rotating disk). A copy of the software also is provided on removable media, either an LS-120 floppy disk or a PCMCIA card, which can be inserted into the router's drive or card slot. Normally, when you power on the router, it runs the copy of the software that is installed on the flash drive.

You might want to upgrade the router software as new features are added or software problems are fixed. You normally obtain new software by downloading the images onto your router or onto another system on your local network. Then you install the software upgrade on the router's flash and hard drives. You can also copy the software onto the removable media.

If the software on the flash, hard disk, or removable media becomes damaged, you can reinstall the software onto those devices.

This chapter discusses the following concepts and terminology related to installing and upgrading the JUNOS software:

- JUNOS Software Distribution on page 75
- Storage Media on page 78
- Boot Devices on page 78
- Boot Sequence on page 79

JUNOS Software Distribution

This section discusses the following topics:

- Software Release Names on page 76
- Package Names on page 76

Software Release Names

A JUNOS software release has a name in the following format:

`JUNOS-m.nZx`

m.n is two integers that represent the software release number; *m* denotes the major release number.

Z is a capital letter that indicates the type of software release. In most cases, it is an R, to indicate that this is released software. If you are involved in testing prereleased software, this letter might be an A (for alpha-level software), B (for beta-level software), or I (a capital letter I; for internal, test, or experimental versions of software).

x represents the version of the major software release.

The following is an example of a software release name:

`JUNOS-5.0R1`

Package Names

A *package* is a collection of files that make up a software component.



All JUNOS software is now delivered in signed packages. Signed packages validate the JUNOS software packages by means of the MD5 authentication algorithm. For more information about signed packages, see the release notes.

These software packages are provided as a single unit, called a *bundle*, which you can use to upgrade all the packages at once. You can also upgrade the packages individually.

A software package has a name in the following format:

`package-name-release.tgz or package-name-release-signed.tgz`

package-name is the name of the package. Examples are `jroute` (the routing package) and `kernel` (the operating system package).

Each JUNOS software release consists of a set of software packages whose names contain the package name and the software release version, and includes the following components:

- Kernel and network tools package, which contains the operating system
- Base package, which contains additions to the operating system
- Routing package, which contains the software that runs on the Routing Engine
- Encryption package, which contains security software (domestic version)
- Packet Forwarding Engine software package
- Documentation package, which contains the documentation for the software

release is the software release number; for example, 5.0R1 or 4.4R1.5.

The following are examples of package names:

```
jroute-5.0R1-signed.tgz
jkernel-5.0R1-signed.tgz
jpfe-5.0R1-signed.tgz
jinstall-5.0R1-signed.tgz
```

When upgrading to a major new release, you must use one of the bundles; do not upgrade packages individually.



Note

If you are upgrading to Release 5.0 from 4.x or downgrading from 5.0 to 4.x, use the jinstall package. Otherwise, use the jbundle package to upgrade to a new release.

Downgrading from Release 5.0 to 4.x might require a two-step process. For more information, see “Upgrade to Release 5.0 or Downgrade from Release 5.0” on page 95.

Two sets of JUNOS software packages are provided: one for customers in the United States and Canada and another for other customers. The worldwide version does not include any capabilities that provide encryption of data leaving the router. Otherwise, the two packages are identical.

Storage Media

The router has three forms of storage media:

- Flash drive, which is a nonrotating drive. When a new router is shipped from the factory, the JUNOS software is preinstalled on the flash drive.
- Hard drive, which is a rotating drive. When a new router is shipped from the factory, the JUNOS software is preinstalled on the hard drive. This drive also is used to store system log files and diagnostic dump files.
- Removable media, either a PCMCIA card or a LS-120MB floppy disk. The removable media that ships with each router contains a copy of the JUNOS software.

Table 2 specifies the router's device names. The device names are displayed when the router boots.

Table 2: Release 5.x Device Names

Device	RE 1.0	RE 2.0	RE 3.0
Flash drive	ad0	ad0	ad0
Hard drive	ad2	ad1	ad1
Removable media	afd0	ad4	ad4

Boot Devices

There are three devices from which the router boots: the flash drive, the hard drive, or a removable medium. Typically, the router boots from the flash disk. The disk from which the router boots is called the *primary boot device*, and the other disk is the *alternate boot device*. The primary boot device is generally the flash disk, and the alternate boot device is generally the hard disk.



Note

If the router boots from an alternate boot device, a yellow alarm lights the LED on the router's craft interface.

For information about chassis conditions that trigger alarms, see "Chassis Conditions That Trigger Alarms" on page 383.

Boot Sequence

Normally, the router boots from the flash disk. If it fails, the router attempts to boot from the hard drive, which is the alternate boot device.

If a removable medium is installed when the router boots, the router attempts to boot the image on it. If the booting fails, the router tries the flash disk and then the hard disk.

If the router boots from an alternate boot device, the JUNOS software displays a message indicating this when you log in to the router. For example, this message shows that the software booted from the hard disk (/dev/ad2s1a):

```
login: username
Password: password
Last login: date on terminal

--- JUNOS 5.0R1 built date
---
--- NOTICE: System is running on alternate media device (/dev/ad2s1a).
```


Chapter 5

Configure the Software Initially

You can configure the router from a system console connected to the router's console port or by using Telnet to access the router remotely.

Before you configure the software for the first time, you need the following information:

- Name of the machine
- Machine's domain name
- IP address and prefix length information for router's management Ethernet interface
- IP address of a default router
- IP address of a DNS server
- Password for the user "root"

To configure the software for the first time, follow these steps:

1. Power on the router. The JUNOS software boots automatically.
2. Log in as the user root. There is no password.
3. Start the command-line interface (CLI):

```
root# cli
root@>
```

4. Enter configuration mode:

```
cli> configure
[edit]
root@#
```

5. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" ").

```
[edit]
root@# set system host-name host-name
```

6. Configure the machine's domain name:

```
[edit]
root@# set system domain-name domain-name
```

7. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

8. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]
root@# set system backup-router address
```

9. Configure the IP address of a DNS server:

```
[edit]
root@# set system name-server address
```

10. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string.

To enter a clear-text password, use the following command to set the root password:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

To enter a password that is already encrypted, use the following command to set the root password:

```
[edit]
root@# set system root-authentication encrypted-password encrypted-password
```

To enter an SSH public string, use the following command to set the root password:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

11. Optionally, display the configuration statements:

```
[edit]
root@ show
system {
    host-name host-name;
    domain-name domain.name;
    backup-router address;
    name-server {
        address;
    }
}
interfaces {
    fxp0 {
        unit 0 {
            family inet {
                address address;
            }
        }
    }
}
```

12. Commit the configuration, which activates the configuration on the router:

```
[edit]  
root@# commit
```

13. If you want to configure additional properties at this time, remain in configuration mode and add the necessary configuration statements. Then commit the changes to activate them on the router:

```
[edit]  
root@host-name# commit
```

14. When you have completed configuring the router, exit from configuration mode:

```
[edit]  
root@host-name# exit  
root@host-name>
```

15. After you have installed the software on the router, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the request system snapshot command to back up the new software onto the /altconfig file system. If you do not issue the request system snapshot command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The request system snapshot command causes the root file system to be backed up to /altroot, and /config to be backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



Note

After you issue this command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Chapter 6

Reinstall the Software

If any of the software becomes damaged, you might want to reinstall it. Also, you might want to periodically upgrade the router software as new features become available or as software problems are fixed. This chapter discusses the following topics related to reinstalling the JUNOS Internet software:

- Prepare to Reinstall the JUNOS Software on page 85
- Reinstall the JUNOS Software on page 85
- Reconfigure the JUNOS Software on page 86

Prepare to Reinstall the JUNOS Software

Before you install the JUNOS software, you must do the following:

1. Copy the existing configuration in the file `/config/juniper.conf` from the router to another system or to removable media. You also might want to copy any backup configurations (the files named `/config/juniper.conf.n`, where *n* is a number from 0 through 9). To copy the files, use the file copy command.
2. Have available the removable medium that shipped with the router (also called a boot floppy). If you do not have a boot floppy, contact customer support.

Reinstall the JUNOS Software

To reinstall the JUNOS software, follow these steps:

1. Insert the removable medium into the router.
2. Reboot the router, either by power-cycling it or by issuing the `request system reboot` command from the command-line interface (CLI).
3. When the software asks the following question, type **y**.

```
WARNING: The installation will erase the contents of your disk. Do you wish
to continue (y/n)?
```

4. The router then copies the software from the removable medium onto your system, occasionally displaying status messages. Copying the software can take up to 10 minutes.
5. Remove the removable medium when prompted. The router then reboots from the primary boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

Reconfigure the JUNOS Software

After you have reinstalled the software, you must copy the router's configuration files back to the router. (You also can configure the router from scratch, as described in "Configure the Software Initially" on page 81.) However, before you can copy the configuration files, you must establish network connectivity.

To reconfigure the software, follow these steps:

1. Log in as root. There is no password.
2. Start the CLI:

```
root# cli
root@>
```

3. Enter configuration mode:

```
cli> configure
[edit]
root@#
```

4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" ").

```
[edit]
root@# set system host-name host-name
```

5. Configure the machine's domain name:

```
[edit]
root@# set system domain-name domain-name
```

6. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]
root@# set system backup-router address
```

8. Configure the IP address of a DNS server:

```
[edit]
root@# set system name-server address
```

9. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string.

To enter a clear-text password, use the following command to set the root password:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

To enter a password that is already encrypted, use the following command to set the root password:

```
[edit]
root@# set system root-authentication encrypted-password encrypted-password
```

To enter an SSH public string, use the following command to set the root password:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

10. Commit the changes:

```
[edit]
root@# commit
```

11. Exit from configuration mode:

```
[edit]
root@# exit
root@>
```

12. To check that the router has network connectivity, issue a ping command to a system on the network:

```
root@> ping address
```

If there is no response, reboot the router.

13. Copy the existing configuration and any backup configurations back onto the router. Place the files in the /config directory. To copy the files, use the file copy command.

14. Load and activate the desired configuration:

```
root@> configure
[edit]
root@# load merge /config/filename or load replace /config/filename
[edit]
root@# commit
```

15. After you have installed the software on the router, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the request system snapshot command to back up the new software onto the /altconfig file system. If you do not issue the request system snapshot command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The request system snapshot command causes the root file system to be backed up to /altroot, and /config to be backed up to /altconfig. The root and /config file systems are on the router's flash drive and the /altroot and /altconfig file systems are on the router's hard drive.



Note

After you issue this command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Chapter 7

Upgrade Software Packages

Each JUNOS software release consists of the following software packages:

- jkernel—Operating system package
- jbase—Additions to the operating system
- jroute—Software that runs on the Routing Engine
- jpfe—Software that runs on the Packet Forwarding Engine
- jdocs—Documentation for the software
- jcrypto—Encryption software (in domestic software only)

The packages are also grouped together in a bundle, which is called jbundle.

Normally, you use the bundle to upgrade all of the software packages at the same time. You also can upgrade them individually. When upgrading to a new release, you must install the bundle; do not upgrade the packages individually.



Note

If you are upgrading to Release 5.0 from 4.x or downgrading from 5.0 to 4.x, use the jinstall package. Otherwise, use the jbundle package to upgrade to a new release.

Downgrading from Release 5.0 to 4.x might require a two-step process. For more information, see “Upgrade to Release 5.0 or Downgrade from Release 5.0” on page 95.

To determine which packages are running on the router and to get information about these packages, use the show version command at the top level of the CLI.

This chapter discusses the following topics:

- Upgrade All Software Packages on page 90
- Upgrade Individual Software Packages on page 93

Upgrade All Software Packages

To upgrade all software packages, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>.

To download the software packages, you must have a service contract and an access account. If you need help obtaining an account, contact your Juniper Networks sales representative or send e-mail to logistics@juniper.net.



Note

We recommend that you upgrade all software packages out-of-band using the console or fxp0 interface because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



Note

After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

3. Copy each software package to the router. We recommend that you copy them to the /var/tmp directory, which is on the rotating medium (hard disk) and is a large file system.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/  
filename /var/tmp/filename
```

4. Add the new software package:

```

user@host> request system software add /var/tmp/jbundle-release-signed.tgz validate

/var/tmp/jbundle-release-domestic-signed.tgz
Checking compatibility with configuration
Initializing...
Using /packages/jbase-release_xyz
Using /var/tmp/jbundle-release_xyz-domestic-signed.tgz
Verified MD5 checksum of /var/chroot/var/tmp/jbundle/jbundle-release_xyz-domestic.tgz
Using /var/chroot/var/tmp/jbundle-signed/jbundle-release-domestic.tgz
Using /var/chroot/var/tmp/jbundle/jbase-release_xyz.tgz
Using /var/chroot/var/tmp/jbundle/jkernel-release_xyz.tgz
Using /var/chroot/var/tmp/jbundle/jcrypto-release_xyz.tgz
Using /var/chroot/var/tmp/jbundle/jpfe-release_xyz.tgz
Using /var/chroot/var/tmp/jbundle/jdocs-release_xyz.tgz
Using /var/chroot/var/tmp/jbundle/jroute-release_xyz.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete
Installing package '/var/tmp/jbundle-release_xyz-domestic-signed.tgz' ...
Verified MD5 checksum of jbundle-release_xyz-domestic.tgz
Adding jbundle...
Verified MD5 checksum of jbase-release_xyz.tgz
Verified MD5 checksum of jboot-release_xyz
Verified MD5 checksum of jcrypto-release_xyz.tgz
Verified MD5 checksum of jdocs-release_xyz.tgz
Verified MD5 checksum of jkernel-release_xyz.tgz
Verified MD5 checksum of jpfe-release_xyz.tgz
Verified MD5 checksum of jroute-release_xyz.tgz
Auto-deleting old jroute...
Auto-deleting old jdocs...
Auto-deleting old jpfe...
Auto-deleting old jcrypto...
Restarting kmd ...
Auto-deleting old jkernel...
Auto-deleting old jbase...
Adding jbase...

WARNING:  A reboot is required to load this software correctly
WARNING:  Use the 'request system reboot' command
WARNING:  when software installation is complete

Adding jkernel...
Mounted jkernel package on /dev/vn2...
Adding jcrypto...
Mounted jcrypto package on /dev/vn6...
Adding jpfe...
Mounted jpfe package on /dev/vn3...
Adding jdocs...
Mounted jdocs package on /dev/vn8...
Adding jroute...
Mounted jroute package on /dev/vn12...
Saving package file in /var/sw/pkg/jbundle-release_xyz-domestic-signed.tgz ...
Saving state for rollback ...

root@host>

```

package-name is the full URL to the file. *release-number* is the major software release number; for example, 4.2R1.

**Note**

The request system software add *package-name* validate command validates *package-name* against the current configuration as a prerequisite to adding the software. For more information about this command, see the *JUNOS Internet Software Guide: Operational Mode Command Reference*.

The request system software *package-name* validate command validates candidate software against the current configuration of the router. For more information about this command, see the *JUNOS Internet Software Guide: Operational Mode Command Reference*.

5. Reboot the router to start the new software:

```
user@host> request system reboot
```

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the request system snapshot command to back up the new software:

```
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.

**Note**

After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Upgrade Individual Software Packages

To upgrade an individual JUNOS software package, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>.

To download the software packages, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks web site, <https://www.juniper.net/registration/Register.jsp>. You can also call Juniper Networks support at 1-888-314-JTAC (from within the United States) 1-408-745-2121 (from outside the United States).



Note

We recommend that you upgrade all individual software packages out-of-band using the console or fxp0 interface because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



Note

After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

3. Copy each software package to the router. You might want to copy them to the /var/tmp directory, which is on the rotating media (hard disk) and is a large file system.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/  
filename /var/tmp/filename
```

4. Add the new software package:

```
user@host> request system software add /var/tmp/package-name-signed.tgz  
Checking available free disk space...11200k available, 6076k suggested.
```

package-name is the full URL to the file.

The system might display the following message:

```
pkg_delete: couldn't entirely delete package
```

This message indicates that someone manually deleted or changed an item that was in a package. You do not need to take any action; the package is still properly deleted.

If you are upgrading more than one package at the same time, add jbase first and the routing software package jroute last. If you are using this procedure to upgrade all packages at once, add them in the following order:

```
user@host> request system software add /var/tmp/jbase-release-signed.tgz
user@host> request system software add /var/tmp/jkernel-release-signed.tgz
user@host> request system software add /var/tmp/jpfe-release-signed.tgz
user@host> request system software add /var/tmp/jdocs-release-signed.tgz
user@host> request system software add /var/tmp/jroute-release-signed.tgz
user@host> request system software add /var/tmp/jcrypto-release-signed.tgz
```

5. Reboot the router to start the new software:

```
user@host> request system reboot
```

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the request system snapshot command to back up the new software.

```
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Chapter 8

Upgrade to Release 5.0 or Downgrade from Release 5.0

The following section is for users who need to upgrade to Release 5.0 from 4.x and downgrade from Release 5.0 to 4.x. The procedure is the same in both cases. To upgrade to Release 5.0 from a 4.x Release, use the 5.0 jinstall package. To downgrade from Release 5.0 to 4.x, use the appropriate 4.x jinstall package.



Note

If you are upgrading to Release 5.0 from 4.x or downgrading from 5.0 to 4.x, use the jinstall package.

If you are upgrading or downgrading from one 5.0 release to another 5.0 release, use the jbundle package. For example, to upgrade from Release 5.0B1 to 5.0B2, use the 5.0B2 jbundle package.



Note

Downgrading from Release 5.0 to 4.x might be a two-step process, depending on the target release:

1. Add the jinstall package for Release 4.x R1.
2. If you need to upgrade from that release to a maintenance release or daily, add the appropriate jbundle package. For example, to downgrade from Release 5.0 to Release 4.4R2.3, add the jinstall package for 4.4R1 and then the jbundle package for 4.4R2.3.

To upgrade to or downgrade from Release 5.0, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>.

To download the software packages, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks web site, <https://www.juniper.net/registration/Register.jsp>. You can also call Juniper Networks support at 1-888-314-JTAC (from within the United States) or 1-408-745-2121 (from outside the United States).



We recommend that you upgrade and downgrade software packages out-of-band using the console or fxp0 interface because in-band connections can be lost during the downgrade or upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



After you issue this command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

3. Copy the jinstall package to the router. You might want to copy them to the /var/tmp directory, which is on the rotating media (hard disk) and is a large file system.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/  
filename /var/tmp/filename
```

4. Add the jinstall package:

```
user@host> request system software add /var/tmp/ jinstall-package-name
Installing package '/var/tmp/jinstall-package-name'...
```

```
WARNING: This package will load JUNOS software release-number.
WARNING: It will save JUNOS configuration files, log files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. This is the pre-installation stage
WARNING: and all the software is loaded when you reboot the system.
```

```
Saving the config files ...
Installing the bootstrap installer ...
```

```
WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING: 'request system reboot' command when software installation is
WARNING: complete. To abort the installation, do not reboot your system,
WARNING: instead use the 'request system software delete jinstall'
WARNING: command as soon as this operation completes.
```

```
Saving package file in /var/sw/pkg/ jinstall-package-name ...
Saving state for rollback ...
```



Note

The installation process removes most stored files (except log, juniper.conf, and ssh files) on the router, such as configuration templates and shell scripts. To preserve these files, copy them to another system before upgrading or downgrading the software.

5. Reboot the router to load the JUNOS software:

```
root@host>request system reboot
Reboot the system ? [yes,no] (no) yes
Shutdown NOW!
```



Note

You must reboot to load the JUNOS software. To reboot, issue the request system reboot command when you are done installing the software.

To abort the installation, do not reboot your system; instead, issue the request system software delete jinstall command when you are done installing the software.

All the software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The router then reboots from the primary boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

6. Log in and verify the version of software running after the router reboots. Issue the show log message or show version command.

7. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the request system snapshot command to back up the new software.

The request system snapshot command causes the root file system to be backed up to /altroot, and /config to be backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



Note

After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.



Note

You cannot issue the request system software rollback command to return to the previously installed software after using a jinstall package.

To return to the previously installed software, use the jinstall package that corresponds with the previously installed software.

Part 3

Command-Line Interface

- Command-Line Interface Overview on page 101
- Command-Line Interface Operational Mode on page 103
- Control the CLI Environment on page 123
- Configure the Router with the CLI on page 127
- Configuration Groups on page 179
- Summary of CLI Environment Commands on page 197
- Summary of CLI Configuration Mode Commands on page 203
- Summary of CLI Operational Mode Commands on page 215

Chapter 9

Command-Line Interface Overview

The command-line interface (CLI) is the interface to the software that you use whenever you access the router—whether from the console or through a remote network connection. The CLI, which automatically starts after the router finishes booting, provides commands that you use to perform various tasks, including configuring the JUNOS software and monitoring and troubleshooting the software, network connectivity, and the router hardware.

The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI provides command help and command completion, and it also provides Emacs-style keyboard sequences that allow you to move around on a command line and scroll through a buffer that contains recently executed commands.

The CLI is indicated by the presence of the > prompt, which is preceded by a string that defaults to the name of the user and the name of the router. For example:

```
user@host>
```

For information about customizing your CLI session, see “Configure the Router with the CLI” on page 127.

This chapter discusses the following topics:

- CLI Modes on page 101
- CLI Command Hierarchy on page 102

CLI Modes

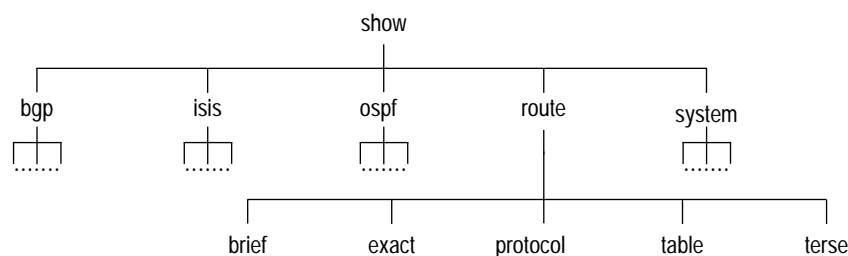
The CLI has two modes: operational and configuration. In operational mode, you monitor and troubleshoot the software, network connectivity, and the router by entering commands. For more information about operational mode, see “Command-Line Interface Operational Mode” on page 103.

When in configuration mode, you configure the JUNOS software by creating a hierarchy of configuration statements. You can do this by using the CLI or by creating a text (ASCII) file that contains the statement hierarchy. (The statement hierarchy is identical in both the CLI and text configuration file.) You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties. When you have finished entering the configuration statements, you commit them, which activates the configuration on the router. For more information about configuration mode, see “Configure the Router with the CLI” on page 127.

CLI Command Hierarchy

The CLI commands are organized in a hierarchical fashion, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the system and the system software are grouped under the `show` command, and all commands that display information about the routing table are grouped under the `show route` command. Figure 2 illustrates a portion of the `show` command hierarchy.

Figure 2: CLI Command Hierarchy Example



To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of the routes in the router table, use the command `show route brief`.

The hierarchical organization results in commands that have a regular syntax and provides several features that simplify CLI use:

- **Consistent command names**—Commands that provide the same type of function have the same name, regardless of the portion of the software they are operating on. As examples, all `show` commands display software information and statistics, and all `clear` commands erase various types of system information.
- **Lists and short descriptions of available commands**—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command. This means that if you already are familiar with the JUNOS software or with other routing software, you can use many of the CLI commands without referring to the documentation.
- **Command completion**—Command completion for command names (keywords) and for command options is also available at each level of the hierarchy. If you type a partial command name followed immediately by a question mark (with no intervening space), you see a list of commands that match the partial name you typed.

Chapter 10

Command-Line Interface Operational Mode

When you log in to the router and the command-line interface (CLI) starts, you are at the top level of operational mode. At this level, there are a number of broad groups of CLI commands:

- **Commands for controlling the CLI environment**—The commands in the set hierarchy configure the CLI display screen. For information about these commands, see “Control the CLI Environment” on page 123.
- **Commands for monitoring and troubleshooting**—The following commands let you display information and statistics about the software and test network connectivity. Using these commands is discussed in the *JUNOS Internet Software Operational Mode Command Reference*.
 - **clear**—Clear statistics and protocol database information.
 - **mtrace**—Trace mtrace packets from source to receiver.
 - **monitor**—Perform real-time debugging of various software components, including the routing protocols and interfaces.
 - **ping**—Determine the reachability of a remote network host.
 - **show**—Display the current configuration and information about interfaces, routing protocols, routing tables, routing policy filters, and the chassis.
 - **test**—Test the configuration and application of policy filters and AS path regular expressions.
 - **traceroute**—Trace the route to a remote network host.
- **Commands for connecting to other network systems**—The **ssh** command opens secure shell connections, and the **telnet** command opens Telnet sessions to other hosts on the network. For information about these commands, see the *JUNOS Internet Software Operational Mode Command Reference*.
- **Commands for copying files**—The **file** and **copy** commands copy files from one location on the router to another, from the router to a remote system, or from a remote system to the router. For information about these commands, see the *JUNOS Internet Software Operational Mode Command Reference*.
- **Commands for restarting software processes**—The commands in the **restart** hierarchy restart the various JUNOS software processes, including the routing protocol, interface, and SNMP. For information about these commands, see the *JUNOS Internet Software Operational Mode Command Reference*.

- A command—request—for performing system-level operations, including stopping and rebooting the router and loading JUNOS software images. For information about this command, see the *JUNOS Internet Software Operational Mode Command Reference*.
- A command—start—to exit the CLI and start a UNIX shell. For information about this command, see the *JUNOS Internet Software Operational Mode Command Reference*.
- A command—configure—for entering configuration mode, which provides a series of commands that configure the JUNOS software, including the routing protocols, interfaces, network management, and user access. For information about the CLI configuration commands, see “Configure the Router with the CLI” on page 127.
- A command—quit—to exit the CLI. For information about this command, see the *JUNOS Internet Software Operational Mode Command Reference*.

For more information about the CLI operational mode commands, see the *JUNOS Internet Software Operational Mode Command Reference*.

This chapter discusses the following topics about the CLI:

- Use the CLI on page 104
- Set the Current Date and Time on page 119
- Set Date and Time from NTP Servers on page 119
- Display CLI Command History on page 120
- Monitor Who Uses the CLI on page 121

Use the CLI

This section describes how to use the JUNOS software CLI. It discusses the following topics:

- Get Help About Commands on page 105
- Have the CLI Complete Commands on page 106
- CLI Messages on page 107
- Move around and Edit the Command Line on page 108
- How Output Appears on the Screen on page 109

Get Help About Commands

The CLI provides context-sensitive help at every level of the command hierarchy. The help information tells you which commands are available at the current level in the hierarchy and provides a brief description of each.

To get help while in the CLI, type ?. You do not need to press Enter after typing the question mark.

- If you type the question mark at the command-line prompt, the CLI lists the available commands and options.
- If you type the question mark after entering the complete name of a command or command option, the CLI lists the available commands and options, then redisplay the command names and options that you typed.
- If you type the question mark in the middle of a command name, the CLI lists possible command completions that match the letters you have entered so far, then redisplay the letters that you typed.

Examples: Get Help About Commands

List all available commands at the top level of the CLI's operational mode:

```
user@host> ?
Possible completions:
clear          Clear information in the system
configure      Manipulate software configuration information
file           Perform file operations
help           Provide help information
mtrace         Trace mtrace packets from source to receiver.
monitor        Real-time debugging
ping           Ping a remote target
quit           Exit the management session
request        Make system-level requests
restart        Restart a software process
set            Set CLI properties, date, time, craft display text
show           Show information about the system
ssh            Open a secure shell to another host
start          Start a software process
telnet         Telnet to another host
test           Diagnostic debugging commands
traceroute     Trace the route to a remote host
user@host>
```

List all commands that start with the letter c:

```
user@host> c?
Possible completions:
clear          Clear information in the system
configure      Manipulate software configuration information
user@host> c
```

List all available clear commands:

```
user@host> clear ?
Possible completions:
arp          Clear address-resolution information
bgp          Clear BGP information
chassis      Clear chassis information
firewall     Clear firewall counters
igmp         Clear IGMP information
interfaces   Clear interface information
ilmi         Clear ILMI statistics information
isis         Clear IS-IS information
ldp          Clear LDP information
log          Clear contents of a log file
mpls         Clear MPLS information
msdp         Clear MSDP information
multicast    Clear Multicast information
ospf         Clear OSPF information
pim          Clear PIM information
rip          Clear RIP information
route        Clear routing table information
rsvp         Clear RSVP information
snmp         Clear SNMP information
system       Clear system status
vrrp         Clear VRRP statistics information
user@host> clear
```

Have the CLI Complete Commands

You do not always have to remember or type the full command or option name for the CLI to recognize it. To display all possible command or option completions, type the partial command followed immediately by a question mark.

To complete a command or option that you have partially typed, press the tab key or the spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command, and the possible completions are displayed.

Command completion also applies to other strings, such as filenames and usernames. To display all possible values, type a partial string followed immediately by a question mark. However, to complete these strings, press the tab key; pressing the space bar does not work.

Examples: Use CLI Command Completion

Issue the show interfaces command:

```
user@host> sh<Space>ow i<Space>
'i' is ambiguous.
Possible completions:
  igmp      Show information about IGMP
  interface Show interface information
  isis      Show information about IS-IS
user@host> show in<Space>terfaces <Enter>
Physical interface: at-0/1/0, Enabled, Physical link is Up
Interface index: 11, SNMP ifIndex: 65
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode
Speed: OC12, Loopback: None, Payload scrambler: Enabled
Device flags   : Present Running
Link flags     : 0x01
...
user@host>
```

Display a list of all log files whose names start with the string “messages,” and then display the contents of one of the files:

```
user@myhost> show log mes?
Possible completions:
<filename>      Log file to display
messages        Size: 1417052, Last changed: Mar  3 00:33
messages.0.gz   Size: 145575, Last changed: Mar  3 00:00
messages.1.gz   Size: 134253, Last changed: Mar  2 23:00
messages.10.gz  Size: 137022, Last changed: Mar  2 14:00
messages.2.gr   Size: 137112, Last changed: Mar  2 22:00
messages.3.gz   Size: 121633, Last changed: Mar  2 21:00
messages.4.gz   Size: 135715, Last changed: Mar  2 20:00
messages.5.gz   Size: 137504, Last changed: Mar  2 19:00
messages.6.gz   Size: 134591, Last changed: Mar  2 18:00
messages.7.gz   Size: 132670, Last changed: Mar  2 17:00
messages.8.gz   Size: 136596, Last changed: Mar  2 16:00
messages.9.gz   Size: 136210, Last changed: Mar  2 15:00
user@myhost> show log mes<Tab>sages.4<Tab>.gz<Enter>
Jan 15 21:00:00 myhost newsyslog[1381]: logfile turned over
...
```

CLI Messages

Messages appear when you enter and exit from configuration mode, when you commit a configuration, and when you type a string or value that is not valid.

When you commit a configuration, the JUNOS software checks the configuration you are committing. If there are no problems, a message indicates that the configuration was accepted. If there are problems, a message indicates where the errors are.

In the top-level CLI commands and in configuration mode, if you type an invalid string—for example, the name of a command or statement that does not exist—you see the message “syntax error” or “unknown command.” A caret (^) indicates where the error is. Examples:

```
user@host> clear route
                        ^
syntax error, expecting <command>.

[edit]
user@host# telnet
                ^
unknown command.
```

When the number of choices is limited, a message might display the commands you can enter to correct the syntax error. For example,

```
[edit]
user@host# load myconfig-file<Enter>
                ^
syntax error, expecting 'merge', 'override', or 'replace'.
```

Move around and Edit the Command Line

In the CLI, you can use keyboard sequences to move around on a command line and edit the command line. You can also use keyboard sequences to scroll through a list of recently executed commands. Table 3 lists some of the CLI keyboard sequences. They are the same as those used in Emacs.

Table 3: CLI Keyboard Sequences

Category	Action	Keyboard Sequence
Move the Cursor	Move the cursor back one character.	Ctrl-b
	Move the cursor back one word.	Esc-b or Alt-b
	Move the cursor forward one character.	Ctrl-f
	Move the cursor forward one word.	Esc-f or Alt-f
	Move the cursor to the beginning of the command line.	Ctrl-a
	Move the cursor to the end of the command line.	Ctrl-e
Delete Characters	Delete the character before the cursor.	Ctrl-h, Delete, or Backspace
	Delete the character at the cursor.	Ctrl-d
	Delete all characters from the cursor to the end of the command line.	Ctrl-k
	Delete all characters on the command line.	Ctrl-u or Ctrl-x
	Delete the word before the cursor.	Ctrl-w, Esc-Backspace, or Alt-Backspace
	Delete the word after the cursor.	Esc-d or Alt-d
Insert Recently Deleted Text	Insert the most recently deleted text at the cursor.	Ctrl-y

Category	Action	Keyboard Sequence
Redraw the Screen	Redraw the current line.	Ctrl-l
Display Previous Command Lines	Scroll backward through the list of recently executed commands.	Ctrl-p
	Scroll forward through the list of recently executed commands.	Ctrl-n
	Search the CLI history in reverse order for lines matching the search string.	Ctrl-r
	Search the CLI history by typing some text at the prompt, followed by the keyboard sequence. The CLI attempts to expand the text into the most recent word in the history for which the text is a prefix.	Esc-/
Repeat Keyboard Sequences	Specify the number of times to execute a keyboard sequence. <i>number</i> can be from 1 through 9.	Esc- <i>number</i> sequence or Alt- <i>number</i> sequence

How Output Appears on the Screen

When you issue commands in operational mode, or when you issue the `show` command in configuration mode, the output appears on the screen. You can also filter the output of commands, either to perform simple commands on the output or to place the output into a file.

This section discusses the following topics:

- Display Output One Screen at a Time on page 109
- Filter Command Output on page 110

Display Output One Screen at a Time

If the output is longer than the screen length, it appears one screen at a time using a UNIX more-type interface. The prompt `--More--` indicates that more output is available. Table 4 lists the keyboard sequences you can use at the `--More--` prompt. As soon as the CLI knows how long the output is (usually by the second screen), it displays the percentage of the command output above the prompt.

Table 4: `--More--` Prompt Keyboard Sequences

Category	Action	Keyboard Sequence
Get Help	Display information about the keyboard sequences you can display at the <code>--More--</code> prompt.	h
Scroll Down	Scroll down one line.	Enter, Return, k, Ctrl-m, Ctrl-n, or down arrow
	Scroll down one-half screen.	Tab, d, Ctrl-d, or Ctrl-x
	Scroll down one whole screen.	Space or Ctrl-f
	Scroll down to the bottom of the output.	Ctrl-e or G
	Display the output all at once instead of one screen at a time. (Same as specifying the <code> no-more</code> command.)	N

Category	Action	Keyboard Sequence
Scroll Up	Display the previous line of output.	j, Ctrl-h, Ctrl-p, or up arrow
	Scroll up one-half screen.	u or Ctrl-u
	Scroll up one whole screen.	b or Ctrl-b
	Scroll up to the top of the output.	Ctrl-a or g
Search	Search forward for a string.	/string
	Search backward for a string.	?string
	Repeat the previous search for a string.	n
	Search for a text string. You are prompted for the string to match. (Same as specifying the match string command.)	m or M
	Search, ignoring a text string. You are prompted for the string to not match. (Same as specifying the except string command.)	e or E
Interrupt or End Output, Redraw the Output, and Save the Output to a File	Interrupt the display of output.	Ctrl-C, q, Q, or Ctrl-k
	Do not redisplay the CLI prompt immediately after displaying the output, but remain at the ---More--- prompt. (Same as specifying the hold command.)	H
	Clear any match conditions and display the complete output.	c or C
	Redraw the output on the screen.	Ctrl-l
	Save the command output to a file. You are prompted for a filename. (Same as specifying the save filename command.)	s or S

Filter Command Output

For operational and configuration commands that display output, such as the show commands, you can filter the output. When you display help about these commands, one of the options listed is |, called a *pipe*, which allows you to filter the command output. For example:

```

user@host> show configuration ?
Possible completions:
  <[Enter]> Execute this command
  |       Pipe through a command
user@host> show configuration | ?
Possible completions:
count      Count occurrences
except     Show only text that does not match a pattern
find       Search for the first occurrence of a pattern
hold       Hold text without exiting the ---More--- prompt
match      Show only text that matches a pattern
no-more    Don't paginate output
resolve    Resolve IP addresses
save       Save output text to a file
trim       Trim specified number of columns from the start line

```

In configuration mode, two additional filters appear, display and compare:

```
[edit]
user@host # show | ?
Possible completions:
  compare  Compare configuration changes with a prior version
  count    Count occurrences
  display  Display additional configuration information
  except   Show only text that does not match a pattern
  find     Search for the first occurrence of a pattern
  hold     Hold text without exiting the ---More--- prompt
  match    Show only text that matches a pattern
  no-more  Don't paginate output
  resolve  Resolve IP addresses
  save     Save output text to a file
  trim     Trim specified number of columns from the start line
```

The following filtering operations are available:

- Place Command Output in a File on page 111
- Search for a String in the Output on page 112
- Compare Configuration Changes with a Prior Version on page 114
- Count the Number of Lines in the Output on page 116
- Display All Output at Once on page 116
- Retain the Output after the Last Screen on page 116
- Display Additional Information about the Configuration on page 116
- Filter Command Output Multiple Times on page 119

Place Command Output in a File

When the output is very long, when you need to store or analyze the output, or when you need to email or FTP the output, you can place the output of a command into a file. Doing this is useful when the output scrolls off the screen, making it difficult to cut the output from a window and paste it into another.

To save the output to a file, specify the save command after the pipe:

```
user@host> command | save filename
```

By default, the file is placed in your home directory on the router. For information about how you can specify the name of the file, see “How to Specify Filenames and URLs” on page 224.

This example stores the output of the request support information command in a file:

```
user@host> request support information | save filename
Wrote 1143 lines of output to 'filename'
user@host>
```

Search for a String in the Output

You can search for text matching a regular expression by filtering output. You can make a regular expression match everything except a regular expression, or find the first occurrence of text matching a regular expression. Searches are not case-sensitive.

To match a regular expression, specify the match command after the pipe:

```
user@host> command | match regular-expression
```

To ignore text that matches a regular expression, specify the except command after the pipe:

```
user@host> command | except regular-expression
```

If the *regular-expression* contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

You use extended regular expressions to specify what text in the output to match. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 5 lists common regular expression operators.

Table 5: Common Regular Expression Operators

Operator	Match...
	One of the two terms on either side of the pipe.
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces \$" means that the user cannot issue show interfaces detail or show interfaces extensive.
[]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
()	A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression.

For example, if a command produces the following output:

```
one two
two two
three two one
four
```

The match two command displays:

```
one two
two two
three two one
```

The except one command displays:

```
two two
four
```

List all the ATM interfaces in the configuration:

```
user@host> show configuration | match at-
at-2/1/0 {
at-2/1/1 {
at-2/2/0 {
at-5/2/0 {
at-5/3/0 {
```

Display a skeleton of your router configuration:

```
[edit]
user@host # show | match {
system {
  root-authentication {
  name-server {
  login {
    class superuser {
    user juniper {
      authentication {
  services {
  syslog {
    file messages {
  processes {
chassis {
  alarm {
    sonet {
  images {
    scb {
    fpc {
interfaces {
  at-2/1/1 {
    atm-options {
    unit 0 {
  at-2/2/0 {
  ...
snmp {
  community public {
  clients {
routing-options {
  static {
    route 0.0.0.0/0 {
    route 192.168.0.0/16 {
    route 208.197.169.0/24 {
protocols {
  rsvp {
    interface so-5/1/0 {
  mpls {
    interface so-5/1/0 {
  bgp {
    group internal {
  ospf {
    area 0.0.0.0 {
      interface so-5/1/0 {
```

List all users who are logged into the router except for the user “root”:

```
user@host> show system users | except root
8:28PM up 1 day, 13:59, 2 users, load averages: 0.01, 0.01, 0.00
USER  TTY FROM          LOGIN@  IDLE WHAT
sheep  p0  baa.juniper.net  7:25PM  - cli
```

Save the configuration, except for encrypted passwords, to a file:

```
user@host> show configuration | except SECRET-DATA | save my.output.file
```

Display the output, starting not at the beginning but rather at the first occurrence of text matching a regular expression, using the find command after the pipe:

```
user@host> command | find regular-expression
```

If the regular expression contains spaces, operators, or wildcard characters, enclose the expression in quotation marks.

List the routes in the routing table starting at 208.197.169.0:

```
user@host> show route | find 208.197.169.0
208.197.169.0/24    *[Static/5] 1d 13:22:11
                  > to 192.168.4.254 via so-3/0/0.0
224.0.0.5/32      *[OSPF/10] 1d 13:22:12, metric 1

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.1921.6800.4015.00/160
                  *[Direct/0] 1d 13:22:12
                  > via lo0.0
```

Compare Configuration Changes with a Prior Version

In configuration mode only, when you have made changes to the configuration and want to compare the candidate configuration with a prior version, you can use the compare command to display the configuration. The compare command compares the candidate configuration with either the current committed configuration or a configuration file and displays the differences between the two configurations. To compare configurations, specify the compare command after the pipe:

```
[edit]
user@host# show | compare [filename | rollback n]
```

filename is the full path to a configuration file. The file must be in the proper format: a hierarchy of statements. For information about how to save a configuration to a file, see “Save a Configuration to a File” on page 161. For information about formatting the hierarchy of statements, see “Configuration Statement Hierarchy” on page 128.

n is the index into the list of previously committed configurations. The most recently saved configuration is number 0, and the oldest saved configuration is number 9. If you do not specify arguments, the candidate configuration is compared against the active configuration file (/config/juniper.conf).

The comparison output uses the following conventions:

- Statements that are only in the candidate configuration are prefixed with a plus sign (+).
- Statements that are only in the comparison file are prefixed with a minus sign (-).
- Statements that are unchanged are prefixed with a single blank space ().

The following example shows various changes, then a comparison of the candidate configuration with the active configuration, showing only the changes made at the [edit protocols bgp] hierarchy level.

```
[edit]
user@host# edit protocols bgp

[edit protocols bgp]
user@host# show
group my-group {
    type internal;
    hold-time 60;
    advertise-inactive;
    allow 1.1.1.1/32;
}
group fred {
    type external;
    peer-as 33333;
    allow 2.2.2.2/32;
}
group test-peers {
    type external;
    allow 3.3.3.3/32;
}
[edit protocols bgp]
user@host# set group my-group hold-time 90
[edit protocols bgp]
user@host# delete group my-group advertise-inactive
[edit protocols bgp]
user@host# set group fred advertise-inactive
[edit protocols bgp]
user@host# delete group test-peers
[edit protocols bgp]
user@host# show | compare
[edit protocols bgp group my-group]
- hold-time 60;
+ hold-time 90;
- advertise-inactive;
[edit protocols bgp group fred]
+ advertise-inactive;
[edit protocols bgp]
-group test-peers {
- type external;
- allow 3.3.3.3/32;
-}
[edit protocols bgp]
user@host# show
group my-group {
    type internal;
    hold-time 90;
    allow 1.1.1.1/32;
}
group fred {
    type external;
    advertise-inactive;
    peer-as 33333;
    allow 2.2.2.2/32;
}
```

Count the Number of Lines in the Output

To count the number of lines in the output, specify the count command after the pipe:

```
user@host> command | count
```

For example:

```
user@host> show configuration | count
Count: 269 lines
user@host> show route | count
Count: 67 lines
```

Display All Output at Once

To display the output all at once instead of one screen at a time, specify the no-more command after the pipe. This command is equivalent to the set cli screen-length 0 command, but affects the output of the one command only.

```
user@host> command | no-more
```

Retain the Output after the Last Screen

When you view output one screen at a time, you typically return to the CLI prompt after viewing the last screen.

To not return immediately, use the hold command after the pipe. This feature is useful, for example, when you want to scroll or search through the output.

```
user@host> command | hold
```

Display Additional Information about the Configuration

In configuration mode only, to display additional information about the configuration, use the display detail command after the pipe in conjunction with a show command. The additional information includes the help string that explains each configuration statement and the permission bits required to add and modify the configuration statement.

```
user@host> show <hierarchy-level> | display detail
```

For example:

```
[edit]
user@host> show | display detail
##
## version: Software version information
## require: system
##
version "3.4R1 [tlim]";
```



```

system {
##
## host-name: Host name for this router
## match: ^[:alnum:]._-]+$
## require: system
##
host-name router-name;
##
## domain-name: Domain name for this router
## match: ^[:alnum:]._-]+$
## require: system
##
domain-name isp.net;
##
## backup-router: Address of router to use while booting
##
backup-router 192.168.100.1;
root-authentication {
##
## encrypted-password: Crypted password string
##
encrypted-password "$1$BYJQE$/ocQof8pmcm7MSGK0"; # SECRET-DATA
}
##
## name-server: DNS name servers
## require: system
##
name-server {
##
## name-server: DNS name server address
##
208.197.1.0;
}
login {
##
## class: User name (login)
## match: ^[:alnum:]._-]+$
##
class superuser {
##
## permissions: Set of permitted operation categories
##
permissions all;
}
...
##
## services: System services
## require: system
##
services {
## services: Service name
##
ftp;
##
## services: Service name
##
telnet;
##
}

```

```

syslog {
  ##
  ## file-name: File to record logging data
  ##
  file messages {
    ##
    ## Facility type
    ## Level name
    ##
    any notice;
    ##
    ## Facility type
    ## Level name
    ##
    authorization info;
  }
}
chassis {
  alarm {
    sonet {
      ##
      ## lol: Loss of light
      ## alias: loss-of-light
      ##
      lol red;
    }
  }
}
interfaces {
  ##
  ## Interface name
  ##
  at-2/1/1 {
    atm-options {
      ##
      ## vpi: Virtual path index
      ## range: 0 .. 255
      ## maximum-vcs: Maximum number of virtual circuits on this VP
      ##
      vpi 0 maximum-vcs 512;
    }
    ##
    ## unit: Logical unit number
    ## range: 0 .. 16384
    ##
    unit 0 {
      ##
      ## vci: ATM point-to-point virtual circuit identifier ([vpi.]vci)
      ## match: ^([[:digit:]]+)(0,1)[[:digit:]]+$
      ##
      vci 0.128;
    }
  }
}
...

```

Filter Command Output Multiple Times

For the output of a single command, you can filter the output one or more times. For example:

```
user@host> command | match regular-expression | except regular-expression | match
other-regular-expression | find regular-expression | hold
```

Set the Current Date and Time

To set the current date and time on the router, use the set date command:

```
user@host> set date YYYYMMDDhhmm.ss
```

YYYY is the four-digit year, MM is the two-digit month, DD is the two-digit date, hh is the two-digit hour, mm is the two-digit minute, and ss is the two-digit second. At a minimum, you must specify the two-digit minute. All other parts of the date and time are optional.

To set the time zone, see “Set the Time Zone” on page 265. To configure time synchronization, see “Configure the Network Time Protocol” on page 266.

Set Date and Time from NTP Servers

If the NTP server is unable to synchronize the current date and time on the router, a system log message similar to the following appears:

```
"time error %.Of over %d seconds; set clock manually".
```

To set the date and time from all NTP servers configured at the [edit system ntp server] hierarchy level to determine the correct time, use the set date ntp command:

```
user@host> set date ntp
```



Note

You do not need to reboot the router when you use the set date ntp command.

To set the date and time from a NTP server configured at the [edit system ntp server] hierarchy level to determine the correct time, use the set date ntp command:

```
user@host> set date ntp <ntp-server>
```

To set the date and time from multiple NTP servers configured at the [edit system ntp server] hierarchy level to determine the correct time, use the set date ntp command:

```
user@host> set date ntp <ntp-server>
```

ntp-server—IP address of one or more NTP servers to query. When querying more than one server, enclose the IP addresses in quotes using the format "*ip-address ip-address*". For example:

```
user@host> set date ntp "200.49.40.1 129.127.28.4"
10 Feb 13:50:21 ntpdate[794]: step time server 129.127.28.4 offset 0.000163 sec
```

For more information about how to configure the Network Time Protocol, see "Configure the Network Time Protocol" on page 266 and the *JUNOS Internet Software Command Reference*.

Display CLI Command History

You can display a list of recent commands that you issued. To display the command history, use the show cli history command:

```
user@host> show cli history
03-03 01:00:50 -- show cli history
03-03 01:01:12 -- show interfaces terse
03-03 01:01:22 -- show interfaces lo0
03-03 01:01:44 -- show bgp next-hop-database
03-03 01:01:51 -- show cli history
```

By default, this command displays the last 100 commands issued in the CLI. If you specify a number with the command, it displays that number of recent commands. For example:

```
user@host> show cli history 3
01:01:44 -- show bgp next-hop-database
01:01:51 -- show cli history
01:02:51 -- show cli history 3
```

Monitor Who Uses the CLI

Depending upon how you configure the JUNOS software, multiple users can log in to the router, use the CLI, and configure or modify the software configuration.

The JUNOS software provides a general syslog-like mechanism to log system operations, such as when users log in to the router and when they issue CLI commands. To configure system logging, include the `syslog` statement in the configuration, as described in the section “Configure System Logging” on page 271.

If, when you enter configuration mode, another user is also in configuration mode, a notification message is displayed that indicates who the user is and what portion of the configuration they are viewing or editing:

```
user@host> configure
Entering configuration mode
Current configuration users:
  root terminal p3 (pid 1088) on since 1999-05-13 01:03:27 EDT
    [edit interfaces so-3/0/0 unit 0 family inet]
The configuration has been changed but not committed
```

.....

Chapter 11

Control the CLI Environment

To configure the command-line interface (CLI) environment, use the operational-mode CLI set command:

```
user@host> set cli ?
Possible completions:
  complete-on-space  Toggle word completion on space
  idle-timeout       Set the cli maximum idle time
  prompt            Set the cli command prompt string
  restart-on-upgrade Set cli to prompt for restart after a software upgrade
  screen-length      Set number of lines on screen
  screen-width       Set number of characters on a line
  terminal           Set terminal type
```

When you log in to the router using ssh, or log in from the console when its terminal type is already configured (as described in “Configure Console and Auxiliary Port Properties” on page 277), your terminal type, screen length, and screen width are already set, so you do not need to change them.

This chapter discusses the following topics:

- Set the Terminal Type on page 124
- Set the Screen Length on page 124
- Set the Screen Width on page 124
- Set the CLI Prompt on page 124
- Set the Idle Timeout on page 124
- Set CLI to Prompt after a Software Upgrade on page 125
- Set Command Completion on page 125
- Display CLI Settings on page 125
- Example: Control the CLI Environment on page 125

Set the Terminal Type

To set the terminal type, use the `set cli terminal` command:

```
user@host> set cli terminal terminal-type
```

The *terminal-type* can be one of the following: `ansi`, `vt100`, `small-xterm`, or `xterm`.

Set the Screen Length

The default CLI screen length is 24 lines. To change the length, use the `set cli screen-length` command:

```
user@host> set cli screen-length length
```

Setting the screen length to 0 lines disables the display of output one screen at a time. Disabling this UNIX more-type interface can be useful when you are issuing CLI commands from scripts.

Set the Screen Width

The default CLI screen width is 80 columns. To change the width, use the `set cli screen-width` command:

```
user@host> set cli screen-width width
```

Set the CLI Prompt

The default CLI prompt is `user@host>`. To change this, use the `set cli prompt` command. If the prompt string contains spaces, enclose the string in quotation marks (" ").

```
user@host> set cli prompt string
```

Set the Idle Timeout

By default, an individual CLI session never times out after extended times, unless the `idle-timeout` statement has been included in the user's login class configuration. To set the maximum time an individual session can be idle before the user is logged off the router, use the `set cli idle-timeout` command:

```
user@host> set cli idle-timeout timeout
```

timeout can be 0 through 100,000 minutes. Setting *timeout* to 0 disables the timeout.

Set CLI to Prompt after a Software Upgrade

By default, the CLI prompts you to restart after a software upgrade. To disable the prompt for an individual session, use the `set cli restart-on-upgrade off` command:

```
user@host> set cli restart-on-upgrade off
```

To re-enable the prompt, use the `set cli restart-on-upgrade on` command:

```
user@host> set cli restart-on-upgrade on
```

Set Command Completion

By default, you can press the spacebar or tab key to have the CLI complete a command.

To have the CLI allow only a tab to complete a command, use the `set cli complete-on-space off` command:

```
user@host> set cli complete-on-space off
Disabling complete-on-space
user@host>
```

To reenable the use of both spaces and tabs for command completion, use the `set cli complete-on-space on` command:

```
user@host> set cli complete-on-space on
Enabling complete-on-space
user@host>
```

Display CLI Settings

To display the current CLI settings, use the `show cli` command:

```
user@host> show cli
CLI screen length set to 24
CLI screen width set to 80
CLI complete-on-space set to on
```

Example: Control the CLI Environment

Change the default CLI environment:

```
user@host> set cli screen-length 66
Screen length set to 66
user@host> set cli screen-width 40
Screen width set to 40
user@host> set cli prompt "router1-san-jose > "
router1-san-jose > show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen length set to 66
CLI screen width set to 40
CLI terminal is 'xterm'
router1-san-jose >
```

.....

Chapter 12

Configure the Router with the CLI

To configure the router, including the routing protocols, router interfaces, network management, and user access, you must enter a separate mode called configuration mode. Do this by issuing the configure operational mode command.

In configuration mode, the command-line interface (CLI) provides commands to configure the router, load a text (ASCII) file that contains the router configuration, activate a configuration, and save the configuration to a text file.

This chapter discusses the following topics:

- Configuration Statement Hierarchy on page 128
- How the Configuration Is Stored on page 130
- Enter Configuration Mode on page 131
- Configuration Mode Prompt on page 136
- Configuration Mode Banner on page 136
- Configuration Statements and Identifiers on page 136
- Get Help about Configuration Mode Commands, Statements, and Identifiers on page 139
- Create and Modify the Configuration on page 142
- Move among Levels of the Hierarchy on page 145
- Exit Configuration Mode on page 148
- Display the Current Configuration on page 148
- Display Users Currently Editing the Configuration on page 150
- Remove a Statement from the Configuration on page 150
- Copy a Statement in the Configuration on page 152
- Rename an Identifier on page 153
- Insert a New Identifier on page 153
- Run an Operational Mode CLI Command from Configuration Mode on page 156

- Display Configuration Mode Command History on page 156
- Verify a Configuration on page 157
- Commit a Configuration on page 157
- Synchronize Routing Engines on page 160
- Save a Configuration to a File on page 161
- Load a Configuration on page 162
- Return to a Previously Committed Configuration on page 164
- Configuration Mode Error Messages on page 165
- Deactivate and Reactivate Statements and Identifiers in a Configuration on page 166
- Add Comments in a Configuration on page 167
- Have Multiple Users Configure the Software on page 170
- Example: Using the CLI to Configure the Router on page 170
- Additional Details about Specifying Statements and Identifiers on page 176

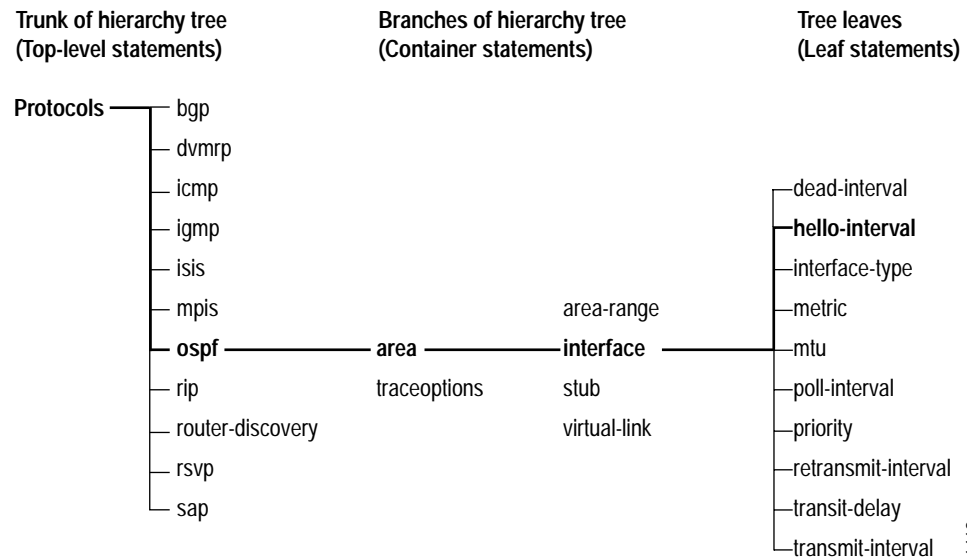
For information about the configuration statements to use to configure particular system functionality, see the chapter about that feature.

Configuration Statement Hierarchy

The JUNOS software configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not contain other statements. All the container and leaf statements together form the *configuration hierarchy*.

Each statement at the top level of the configuration hierarchy resides at the trunk (or root level) of a hierarchy tree. The top-level statements are container statements, containing other statements that form the tree branches. The leaf statements are the leaves of the hierarchy tree. An individual hierarchy of statements, which starts at the trunk of the hierarchy tree, is called a *statement path*. Figure 3 illustrates the hierarchy tree, showing a statement path for the portion of the protocol configuration hierarchy that configures the hello interval on an interface in an OSPF area. The protocols statement is a top-level statement at the trunk of the configuration tree. The ospf, area, and interface statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree), and the hello-interval statement is a leaf on the tree, which, in this case, contains a data value, the length of the hello interval in seconds.

Figure 3: Configuration Mode Hierarchy of Statements



The CLI represents the statement path shown in Figure 3 as [protocols ospf area *area-number* interface *interface-name*], and it displays the configuration as follows:

```

protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
      interface so-0/0/1 {
        hello-interval 5;
      }
    }
  }
}
  
```

The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed. Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon.

The CLI uses this indented representation when it displays the current system configuration, and you use this format when creating ASCII files that contain the software configuration. However, the format of ASCII configuration files is not as strict as the CLI output of the configuration. Although the braces and semicolons are required, the indentation and use of new lines, as shown above, are not required in ASCII configuration files.

How the Configuration Is Stored

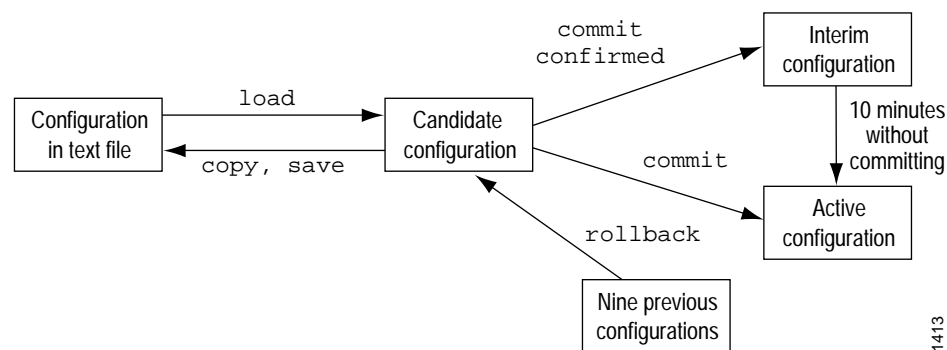
When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible in the CLI immediately, so if multiple users are editing the configuration at the same time, all users can see all changes.

To have a candidate configuration take effect, you *commit* the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

In addition to saving the current configuration, the CLI saves the current operational version and the previous nine versions of committed configurations. The most recently committed configuration is version 0 (the current operational version, which is the default configuration that the system returns to if you roll back to a previous configuration), and the oldest saved configuration is version 9. The currently operational JUNOS software configuration is stored in the file `juniper.conf`, and the last three committed configurations are stored in the files `juniper.conf.1`, `juniper.conf.2`, and `juniper.conf.3`. These four files are located in the directory `/config`, which is on the router's flash drive. The remaining six previous versions of committed configurations, the files `juniper.conf.4` through `juniper.conf.9`, are stored in the directory `/var/db/config` on the hard disk.

Figure 4 illustrates the various router configuration states and the configuration mode commands you use to load, commit, copy, save, or roll back the configuration.

Figure 4: Commands for Storing and Modifying the Router Configuration



1413

Enter Configuration Mode

You enter configuration mode by entering the configure operational mode command.

The following configuration mode commands are available:

```

user@host> configure
entering configuration mode
[edit]
user@host# ?
Possible completions:
<[Enter]>      Execute this command
activate       Remove the inactive tag from a statement
annotate       Annotate the statement with a comment
commit         Commit current set of changes
copy           Copy a statement
deactivate     Add the inactive tag to a statement
delete         Delete a data element
edit           Edit a sub-element
exit           Exit from this level
help           Provide help information
insert         Insert a new ordered data element
load           Load configuration from an ASCII file
quit           Quit from this level
rename         Rename a statement
rollback       Roll back database to last committed version
run            Run an operational-mode command
save           Save configuration to an ASCII file
set            Set a parameter
show           Show a parameter
status         Display database user status
top            Exit to top level of configuration
up             Exit one level of configuration

```

The access privilege level required to enter configuration mode is controlled by the configure permission bit. Users for whom this permission bit is not set do not see the configure command as a possible completion when they enter a ? in operational mode, and they cannot enter configuration mode. Users for whom this bit is set do see this command and can enter configuration mode. When in configuration mode, a user can view and modify only those statements for which they have access privileges set. For more information, see “Configure Access Privilege Levels” on page 254.

This section discusses the following topics:

- Using the Configure Command on page 132
- Using the Configure Exclusive Command on page 132
- Using the Configure Private Command on page 133

Using the Configure Command

If you and other users enter configuration mode with the `configure` command, everyone can make configuration changes and commit all changes made to the configuration. This means that if you and another user have made configuration changes and the other user commits, the changes you made are committed as well. That is, no one has a lockout on the configuration file.

If, when you enter configuration mode, another user is also in configuration mode, a message shows who the user is and what part of the configuration he is viewing or editing:

```
user@host> configure
Entering configuration mode
Current configuration users:
  root terminal p3 (pid 1088) on since 1999-05-13 01:03:27 EDT
    [edit interfaces so-3/0/0 unit 0 family inet]
The configuration has been changed but not committed
[edit]
user@host>
```

If, when you enter configuration mode, the configuration contains changes that have not been committed, a message appears:

```
user@host> configure
Entering configuration mode
The configuration has been changed but not committed
[edit]
user@host>
```

If, while in configuration mode, you try to make a change while the configuration is locked by another user, a message indicates that the configuration database is locked, who the user is, and what portion of the configuration the user is viewing or editing:

```
user@host# set system host-name ipswitch
error: configuration database locked by:
  user2 terminal d0 (pid 1828) on since 19:47:58 EDT, idle 00:02:11
    exclusive [edit protocols]
```

Using the Configure Exclusive Command

If you enter configuration mode with the `configure exclusive` command, you lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. Other users can enter and exit configuration mode, but they cannot change the configuration. If another user has locked the configuration, and you need to forcibly log him or her out, enter the operational mode command `request system logout pid pid_number`. When a user exits from `configure exclusive` mode when another user is in `configure private` mode, the JUNOS software will roll back any uncommitted changes.

If, when you enter configuration mode, another user is also in configuration mode and has locked the configuration, a message indicates who the user is and what portion of the configuration he or she is viewing or editing:

```
user@host> configure
Entering configuration mode
Users currently editing the configuration:
  root terminal p3 (pid 1088) on since 2000-10-30 19:47:58 EDT, idle 00:00:44
    exclusive [edit interfaces so-3/0/0 unit 0 family inet]
```


**Note**

If you are using the configure exclusive command, you cannot exit configuration mode with uncommitted changes while another user is in a configure private session. For more information about the configure private command, see “Using the Configure Private Command” on page 133.

Using the Configure Private Command

The configure private command allows multiple users to edit different parts of the configuration at the same time and to commit only their own changes, or to roll back without interfering with one another’s changes. When you issue the configure private command, you work in a private candidate configuration, which is a copy of the most recently committed configuration.

When you commit a private candidate configuration, the JUNOS software temporarily locks the global configuration, enforces the restriction that the global configuration must be unmodified to commit private changes, and validates the private candidate configuration. If a merge conflict occurs, the commit fails and the configuration lock is released. You can then modify your private candidate configuration and commit it again. If there are no errors, the changes made in the private candidate configuration are merged into the most recently committed global configuration, activated, begin running on the router, and the configuration lock is released.

**Note**

You cannot commit changes in configure private mode when another user is in configure exclusive mode.

If the global configuration has changed, users in configure private mode can issue the rollback or update command to obtain the most recently committed global configuration. For more information about the update command, see “Update the Configure Private Configuration” on page 135.

You must issue the commit command from the top of the configuration.

You cannot save a configure private session; uncommitted changes are discarded.

You cannot issue the commit confirm command when you are in configure private mode.

Users in configure exclusive mode cannot exit configuration mode with uncommitted changes while another user is in configure private mode. A warning message appears notifying the user in configure exclusive mode that his or her changes will be discarded if he or she exits from the configuration.

```
[edit]
user@host# set system host-name fu

[edit]
user@host# quit
The configuration has been changed but not committed
warning: private edits in use. Auto rollback on exiting 'configure exclusive'
Discard uncommitted changes? [yes,no] (yes)

load complete
Exiting configuration mode
user@host
```

When you use the **yes** option to exit configure exclusive mode, the JUNOS software discards your uncommitted changes and rolls back your configuration. The **no** option allows you to continue editing or to commit your changes in configure exclusive mode. These options enforce the restriction that the global configuration must be unmodified for users to commit configure private changes.



You cannot enter configure private mode when the global configuration has been modified.

Note

If a configure private edit is in session, users who issue the configure command can only view the global configuration; a message appears indicating that these users must use the configure exclusive or configure private commands to modify the configuration.

```
[edit]
user@host set system host-name ipswitch
error: private edits in use. Try 'configure private' or 'configure
exclusive'.
[edit]
user@host
```

If the global configuration has been modified, users cannot enter configure private mode because they cannot commit changes when the global configuration has been modified. For example:

```
user@host configure private
error: shared configuration database modified
Users currently editing the configuration:
root terminal d0 (pid 7951) on since 2002-02-21 14:18:46 PST
[edit]
user@host>
```



Users in configure or configure exclusive mode cannot exit the global configuration with uncommitted changes.

Note

If another user commits a change to the same section of the configuration that the private user has modified, a merge conflict may result. The JUNOS software then updates the private user's configuration with the most recently committed global configuration and the private user can commit his or her changes. For example:

```
[edit]
user@host# set system host-name foo

[edit]
user@host# show | compare
[edit system]
- host-name host;
+ host-name foo;

[edit]
user@host# commit
[edit system host-name]
'host-name bar'
statement does not match patch; 'bar' != 'host'
load complete (1 errors)

[edit]
user@host# show | compare
[edit system]
- host-name bar;
+ host-name foo;

[edit]
user@host#
```

In this example, after the JUNOS software detects the merge conflict and fixes it, the user in configure private mode issues the `show | compare` command. This command displays the private user's database changes against the most recently committed global configuration.

Update the Configure Private Configuration

When you are in configure private mode, you must work with a copy of the most recently committed global configuration. If the global configuration changes, you can issue the `update` command to update your private candidate configuration. When you do this, your private candidate configuration contains a copy of the most recently committed configuration with your private changes merged in. For example:

```
[edit]
user@host# update

[edit]
user@host#
```



Note

You can get merge conflicts when you issue the `update` command.

You can also issue the rollback command to discard your private candidate configuration changes and obtain the most recently committed configuration:

```
[edit]
user@host# rollback
```

```
[edit]
user@host#
```

Configuration Mode Prompt

In configuration mode, the prompt changes from a > to a #. For example:

```
user@host> configure
entering configuration mode
[edit]
user@host#
```

Configuration Mode Banner

The portion of the prompt in braces, [edit], is a *banner*. The banner indicates that you are in configuration mode and shows your location in the statement hierarchy. When you first enter configuration mode, you always are at the top level of the hierarchy, which is indicated by the [edit] banner. For example:

```
user@host> configure
enter configuration mode
[edit]
user@host# edit protocols bgp
[edit protocols bgp]
user@host#
```

Top-level banner

Banner at the "protocols bgp" hierarchy level

1463

Configuration Statements and Identifiers

You configure all router properties by including *statements* in the configuration. A statement consists of a keyword, which is fixed text, and, optionally, an *identifier*. An identifier is an identifying name that you define, such as the name of an interface or a user name, and that allows you and the CLI to discriminate among a collection of statements.

The following list shows the statements available at the top level of configuration mode (that is, the trunk of the hierarchy tree). Table 6 on page 137 describes each statement.

user@host# **set ?**

Possible completions:

> accounting-options	Accounting data configuration
+ apply-groups	Groups from which to inherit configuration data
> chassis	Chassis configuration
> class-of-service	Class-of-service configuration
> firewall	Define a firewall configuration
> forwarding-options	Configure options to control packet sampling
> groups	Configuration groups
> interfaces	Interface configuration
> policy-options	Routing policy option configuration
> protocols	Routing protocol configuration
> routing-instances	Routing instance configuration
> routing-options	Protocol-independent routing option configuration
> snmp	Simple Network Management Protocol
> system	System parameters

An angle bracket (>) before the statement name indicates that it is a container statement and that you can define other statements at levels below it.

If there is no angle bracket (>) before the statement name, the statement is a leaf statement; you cannot define other statements at hierarchy levels below it.

A plus sign (+) before the statement name indicates that it can contain a set of values. To specify a set, include the values in brackets. For example:

[edit]

user@host# **set policy-options community my-as1-transit members [65535:10 65535:11]**

In some statements, you can include an identifier. For some identifiers, such as interface names, you must specify the identifier in a precise format. For example, the interface name so-0/0/0 refers to a SONET/SDH interface that is on the FPC in slot 0, in the first PIC location, and in the first port on the PIC. For other identifiers, such as interface descriptive text and policy and firewall term names, you can specify any name, including special characters, spaces, and tabs.

You must enclose in quotation marks (double quotes) identifiers and any strings that include the following characters: space tab () [] { } ! @ # \$ % ^ & | ' = ?

Table 6: Configuration Mode Top-Level Statements

Statement	Description
accounting-options	Configure accounting statistics data collection for interfaces and firewall filters. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Network Management</i> .
chassis	Configure properties of the router chassis, including the clock source, conditions that activate alarms, and SONET/SDH framing and concatenation properties. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
class-of-service	Configure class-of-service parameters. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
firewall	Define filters that select packets based on their contents. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Policy Framework</i> .

Statement	Description
forwarding-options	Define forwarding options, including traffic sampling options. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
groups	Configure configuration groups. For information about statements in this hierarchy, see "Configuration Groups" on page 179.
interfaces	Configure interface information, such as encapsulation, interfaces, virtual channel identifiers (VCIs), and data link channel identifiers (DLCIs). For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
policy-options	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Routing and Routing Protocols</i> .
protocols	Configure routing protocols, including BGP, IS-IS, OSPF, RIP, MPLS, LDP, and RSVP. For information about the statements in this hierarchy, see the chapters that discuss how to configure the individual routing protocols in the <i>JUNOS Internet Software Configuration Guide: Routing and Routing Protocols</i> and the <i>JUNOS Internet Software Configuration Guide: MPLS Applications</i> .
routing-instances	Configure multiple routing instances. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Routing and Routing Protocols</i> .
routing-options	Configure protocol-independent routing options, such as static routes, autonomous system numbers, confederation members, and global tracing (debugging) operations to log. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Routing and Routing Protocols</i> .
snmp	Configure SNMP community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the <i>JUNOS Internet Software Configuration Guide: Network Management</i> .
system	Configure systemwide properties, including the host name, domain name, DNS server, user logins and permissions, mappings between host names and addresses, and software processes. For information about the statements in this hierarchy, see "System Management Configuration Statements" on page 229.

Get Help about Configuration Mode Commands, Statements, and Identifiers

Configuration mode provides two different types of help:

- Use Command Completion in Configuration Mode on page 139
- Get Help Based on a String in a Statement Name on page 141

Use Command Completion in Configuration Mode

The CLI command completion functions described in “Have the CLI Complete Commands” on page 106, which refer to operational mode commands, also apply to the commands in configuration mode and to configuration statements. Specifically, to display all possible commands or statements, type the partial string followed immediately by a question mark, and to complete a command or statement that you have partially typed, press the tab key or spacebar.

Command completion also applies to identifiers, with one slight difference. To display all possible identifiers, type a partial string followed immediately by a question mark. To complete an identifier, you must press the tab key. This scheme allows you to enter identifiers with similar names; then press the spacebar when you are done typing the identifier name.

Examples: Use Command Completion in Configuration Mode

List the configuration mode commands:

```
user@host#?
Possible completions:
<[Enter]>      Execute this command
activate      Remove the inactive tag from a statement
annotate      Annotate the statement with a comment
commit        Commit current set of changes
copy          Copy a statement
deactivate    Add the inactive tag to a statement
delete        Delete a data element
edit          Edit a sub-element
exit          Exit from this level
help          Provide help information
insert        Insert a new ordered data element
load          Load configuration from an ASCII file
quit          Quit from this level
rename        Rename a statement
rollback      Roll back database to last committed version
run           Run an operational-mode command
save          Save configuration to an ASCII file
set           Set a parameter
show          Show a parameter
status        Display database user status
top           Exit to top level of configuration
up            Exit one level of configuration
```

List all the statements available at a particular hierarchy level:

```
[edit]
user@host# edit ?
Possible completions:
> accounting-options  Accounting data configuration
> chassis             Chassis configuration
> class-of-service    Class-of-service configuration
> firewall            Define a firewall configuration
> forwarding-options  Configure options to control packet sampling
> groups              Configuration groups
> interfaces          Interface configuration
> policy-options       Routing policy option configuration
> protocols            Routing protocol configuration
> routing-instances   Routing instance configuration
> routing-options      Protocol-independent routing option configuration
> snmp                Simple Network Management Protocol
> system              System parameters
```

```
user@host# edit protocols ?
Possible completions:
<[Enter]>             Execute this command
> bgp                 BGP options
> connections         Circuit cross-connect configuration
> dvmrp               DVMRP options
> igmp                IGMP options
> isis                IS-IS options
> ldp                 LDP options
> mpls                Multiprotocol Label Switching options
> msdp                MSDP options
> ospf                OSPF configuration
> pim                 PIM options
> rip                 RIP options
> router-discovery    ICMP router discovery options
> rsvp                RSVP options
> sap                 Session Advertisement Protocol options
> vrrp                VRRP options
|                     Pipe through a command
[edit]
user@host# edit protocols
```

List all commands that start with a particular letter or string:

```
user@host# edit routing-options a?
Possible completions:
> aggregate           Coalesced routes
> autonomous-system   Autonomous system number
[edit]
user@host# edit routing-options a
```

List all configured ATM interfaces:

```
user@host# edit interfaces at?
Possible completions:
<interface_name>    Interface name
at-2/1/1
at-2/2/0
at-5/1/0
[edit]
user@host# edit interfaces at
```


Display a list of all configured policy statements:

```
[edit]
user@host# show policy-options policy-statement ?
Possible completions:
<policy_name>      Name to identify a policy filter
[edit]
user@host# show policy-options policy-statement
```

Get Help Based on a String in a Statement Name

In configuration mode, you can use the help command to display help based on a text string contained in a statement name. This command displays help for statements at the current hierarchy level and below.

```
help apropos string
```

string is a text string about which you want to get help. This string is used to match statement names as well as the help strings that are displayed for the statements. If the string contains spaces, enclose it in quotation marks (" "). You also can specify a regular expression for the string, using standard UNIX-style regular expression syntax.

You can also display help based on a text string contained in a statement name using the help topic and help reference commands.

```
help topic string
help reference string
```

The help topic command displays usage guidelines for the statement, while the help reference command displays summary information about the statement.

Example: Get Help Based on a String Contained in a Statement Name

Get help about statements that contain the string “traps”:

```
[edit]
user@host# help apropos traps
set interfaces <interface_name>
  Enable SNMP notifications on state changes
set interfaces <interface_name> unit <interface_unit_number>
  Enable SNMP notifications on state changes
set snmp trap-group
  Configure traps and notifications
set snmp trap-group <group_name> version <version> all
  Send SNMPv1 and SNMPv2 traps
set snmp trap-group <group_name> version <version> v1
  Send SNMPv1 traps
set snmp trap-group <group_name> version <version> v2
  Send SNMPv2 traps
set protocols mpls log-updown
  Send SNMP traps
set firewall filter <filter-name> term <rule-name> from source-port snmptrap
  SNMP traps
set firewall filter <filter-name> term <rule-name> from source-port-except snmptrap
  SNMP traps
set firewall filter <filter-name> term <rule-name> from destination-port snmptrap
  SNMP traps
```

```

set firewall filter <filter-name> term <rule-name> from destination-port-except snmptrap
  SNMP traps
set firewall filter <filter-name> term <rule-name> from port snmptrap
  SNMP traps
set firewall filter <filter-name> term <rule-name> from port-except snmptrap
  SNMP traps
[edit]
user@host# edit interfaces at-5/3/0
[edit interfaces at-5/3/0]
user@host# help apropos traps
set <interface_name>
  Enable SNMP notifications on state changes
set <interface_name> unit <interface_unit_number>
  Enable SNMP notifications on state changes

```

Create and Modify the Configuration

To configure the router or to modify an existing router configuration, you add statements to the configuration, in the process creating a statement hierarchy. For each statement hierarchy, you create the hierarchy starting with a statement at the top level and continuing with statements that move progressively lower in the hierarchy.

For example, to configure an interface in OSPF area 0, you must configure the following hierarchy of statements:

```

protocols
  ospf
    area 0
      interface interface-name

```

To create the hierarchy, you use two configuration mode commands:

- **set**—Creates a statement hierarchy and sets identifier values. After you issue a set command, you remain at the same level in the hierarchy.

The set command has the following syntax:

```
set <statement-path> statement <identifier>
```

statement-path is the hierarchy to the configuration statement and the statement itself. If you have already moved to the statement's hierarchy level, you omit this.

statement is the configuration statement itself.

identifier is a string that identifies an instance of a statement. Not all statements require identifiers. In the example shown at the beginning of this section, the area name and the interface names are identifiers. In many cases, the identifier can contain a space. When you type these identifiers in the configuration, you must enclose them in quotation marks. When the CLI displays these identifiers in the output of a show or other command, it encloses them in quotation marks.

The set command is analogous to an operating system command in which you specify the full path name of the statement you are performing an action on, for example, mkdir /usr/home/boojum/files or mkdir f:\home\boojum\files.

For statements that can have more than one identifier, when you issue a set command to set an identifier, only that identifier is set. The other identifiers that are specified in the statement remain.

- **edit**—Moves to a particular hierarchy level. If that hierarchy level does not exist, the edit command creates it and then moves to it. After you issue an edit command, the banner changes to indicate your current level in the hierarchy.

The edit command has the following general syntax:

```
edit <statement-path> statement <identifier>
```

The edit command is analogous to the combination of operating system commands that you would use to first change to a directory and then perform an action; for example, `cd /usr/home/boojum;mkdir files`.

Examples: Create and Modify the Configuration

To configure an interface to run OSPF, you could issue a single set command from the top level of the configuration hierarchy. The initial [edit] banner indicates that you are at the top level. Notice that after you issue the set command, you remain at the top level of the statement hierarchy, as indicated by the second [edit] banner.

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host#
```

You also can use the edit command to create and move to the [edit protocols ospf area 0.0.0.0 interface so-0/0/0] hierarchy level and then issue a set command to set the value of the hello-interval statement. After you issue the edit command, you move down in the hierarchy, as indicated by the [edit protocols ospf area 0.0.0.0 interface so-0/0/0] banner.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set hello-interval 5
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host#
```

Because hello-interval is an identifier and not a statement, you cannot use the edit command to set the hello interval value. You must use the set command. You can determine that hello-interval is an identifier by listing the available commands at the [edit protocols ospf area 0.0.0.0 interface so-0/0/0] banner. All the statements *not* preceded by a > are identifiers.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
> authentication-key    Authentication key
  dead-interval         Dead interval (seconds)
  disable               Disable OSPF on this interface
  hello-interval        Hello interval (seconds)
  interface-type        Type of interface
  metric                Interface metric (1..65535)
> neighbor              NBMA neighbor
  passive               Do not run OSPF, but advertise it
  poll-interval         Poll interval for NBMA interfaces
  priority               Designated router priority
  retransmit-interval   Retransmission interval (seconds)
  transit-delay         Transit delay (seconds)
  transmit-interval     OSPF packet transmit interval (milliseconds)
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set
```

In both examples above, using either just the set command or a combination of the set and edit commands, you create the same configuration hierarchy:

```
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
```

Notice that the CLI uses indentation to visually represent the hierarchy levels, and it also places braces at the beginning and end of each hierarchy level to set them off. The CLI also places a semicolon at the end of the line that configures the hello-interval statement.

You also use the set command to modify the value of an existing identifier. The following example changes the hello interval in the configuration shown above:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 20
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 20;
      }
    }
  }
}
```

When a statement can have more than one identifier, use the set command to add additional identifiers. Any identifiers that you have already set remain set.

Move among Levels of the Hierarchy

When you first enter configuration mode, you are at the top level of the configuration command hierarchy, which is indicated by the [edit] banner:

```
user@host> configure
entering configuration mode
[edit]
user@host#
```

This section discusses the following topics:

- Move Down to a Specific Level on page 146
- Move Back Up to Your Previous Level on page 146
- Move Up One Level on page 146
- Move Directly to the Top of the Hierarchy on page 147
- Warning Messages When Moving Up on page 147
- Issue Relative Configuration Commands on page 147

Move Down to a Specific Level

To move down through an existing configuration command hierarchy, or to create a hierarchy and move down to that level, use the edit configuration mode command, specifying the hierarchy level at which you want to be. After you issue an edit command, the banner changes to indicate your current level in the hierarchy.

```
edit <statement-path> identifier
```

For example:

```
[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host#
```

Move Back Up to Your Previous Level

To move up the hierarchy, use the exit configuration mode command. This command is, in effect, the opposite of the edit command. That is, the exit command moves you back to your previous level. For example:

```
[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host# edit area 0.0.0.0 interface so-0/0/0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# exit
[edit protocols ospf]
user@host# exit
[edit]
user@host#
```

Move Up One Level

To move up the hierarchy one level at a time, use the up configuration mode command. For example:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set hello-interval 5
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# up
[edit protocols ospf area 0.0.0.0]
user@host# up
[edit protocols ospf]
user@host#
```

Move Directly to the Top of the Hierarchy

To move directly to the top level, use the top configuration mode command. For example:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# top
[edit]
user@host#
```

Warning Messages When Moving Up

If you have omitted a required statement at a particular level, when you issue a show command that displays that hierarchy level, a warning message indicates which statement is missing. For example:

```
[edit protocols mpls]
user@host# set statistics file
[edit protocols mpls]
user@host# show
statistics {
  file; # Warning: missing mandatory statement(s): <filename>
}
interface all;
interface so-3/0/0 {
  disable;
}
```

Issue Relative Configuration Commands

You can issue configuration mode commands from the top of the hierarchy, or from a level above the area you are configuring. This enables you to perform configurations without having move from your current location in the hierarchy. To do this, use the top or up commands followed by another configuration command, including edit, insert, delete, deactivate, annotate, or show.

To issue configuration mode commands from the top of the hierarchy, use the top command; then specify a configuration command. For example:

```
[edit interfaces fxp0 unit 0 family inet]
user@host# top edit system login
[edit system login]
user@host#
```

To issue configuration mode commands from a location higher in the hierarchy, use the up configuration mode command; then specify a configuration command. For example:

```
[edit protocols bgp]
user@host# up 2 activate system
```

Exit Configuration Mode

To exit configuration mode, use the `exit configuration-mode` configuration mode command from any level, or use the `exit` command from the top level. For example:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# exit configuration-mode
exiting configuration mode
user@host>
```

```
[edit]
user@host# exit
exiting configuration mode
user@host>
```

If you try to exit from configuration mode using the `exit` command and the configuration contains changes that have not been committed, you see a message and prompt:

```
[edit]
user@host# exit
The configuration has been changed but not committed
Exit with uncommitted changes? [yes,no] (yes) <Enter>
Exiting configuration mode
user@host>
```

To exit with uncommitted changes without having to respond to a prompt, use the `exit configuration-mode` command. This command is useful when you are using scripts to perform remote configuration.

```
[edit]
user@host# exit configuration-mode
The configuration has been changed but not committed
Exiting configuration mode
user@host>
```

Display the Current Configuration

To display the current configuration, use the `show configuration mode` command. This command displays the configuration at the current hierarchy level or at the specified level.

```
user@host> show <statement-path>
```

When displaying the configuration, the CLI indents each subordinate hierarchy level, inserts braces to indicate the beginning and end of each hierarchy level, and places semicolons at the end of statements that are at the lowest level of the hierarchy. This is the same format that you use when creating an ASCII configuration file, and it is the same format that the CLI uses when saving a configuration to an ASCII file.

The configuration statements appear in a fixed order, and interfaces appear alphabetically by type, and then in numerical order by slot number, PIC number, and port number. Note that when you configure the router, you can enter statements in any order.

You also can use the CLI operational mode `show configuration` command to display the last committed current configuration, which is the configuration currently running on the router:

```
user@host> show configuration
```


If you have omitted a required statement at a particular hierarchy level, when you issue the show command in configuration mode, a message indicates which statement is missing. As long as a mandatory statement is missing, the CLI continues to display this message each time you issue a show command. For example:

```
[edit]
user@host# show
protocols {
  pim {
    interface so-0/0/0 {
      priority 4;
      version 2;
      # Warning: missing mandatory statement(s): 'mode'
    }
  }
}
```

Examples: Display the Current Configuration

Display the entire configuration:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
```

Display a particular hierarchy in the configuration:

```
[edit]
user@host# show protocols ospf area 0.0.0.0
interface so-0/0/0 {
  hello-interval 5;
}
```

Move down to a level and display the configuration at that level:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
  hello-interval 5;
}
```

Display all of the last committed configuration:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host# commit
commit complete
[edit]
user@host# quit
exiting configuration mode
user@host> show configuration
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
```

Display Users Currently Editing the Configuration

To display the users currently editing the configuration, use the status configuration mode command:

```
user@host# status
Current configuration users:
  user terminal p0 (pid 518) on since 2000-03-12 18:24:27 PST
    [edit protocols]
```

The system displays who is editing the configuration (user), from where the user is logged in (terminal p0), the date and time the user logged in (2000-03-12 18:24:27 PST), and what level of the hierarchy the user is editing ([edit protocols]).

Remove a Statement from the Configuration

To delete a statement or identifier, use the delete configuration mode command. Deleting a statement or an identifier effectively “unconfigures” the functionality associated with that statement or identifier, returning that functionality to its default condition.

```
delete <statement-path> <identifier>
```

When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration.

For statements that can have more than one identifier, when you delete one identifier, only that identifier is deleted. The other identifiers in the statement remain.

To delete the entire hierarchy starting at the current hierarchy level, do not specify a statement or an identifier in the delete command. When you omit the statement or identifier, a prompt appears asking you to confirm the deletion:

```
[edit]
user@host# delete
Delete everything under this level? [yes, no] (no) ?
Possible completions:
no      Don't delete everything under this level
yes     Delete everything under this level
Delete everything under this level? [yes, no] (no)
```

Examples: Remove a Statement from the Configuration

Delete the ospf statement, effectively unconfiguring OSPF on the router:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
[edit]
user@host# delete protocols ospf
[edit]
user@host# show
[edit]
user@host#
```

Delete all statements from the current level down:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# set interface so-0/0/0 hello-interval 5
[edit protocols ospf area 0.0.0.0]
user@host# delete
Delete everything under this level? [yes, no] (no) yes
[edit protocols ospf area 0.0.0.0]
user@host# show
[edit]
user@host#
```

Unconfigure a particular property:

```
[edit]
user@host# set interfaces so-3/0/0 speed 100mb
[edit]
user@host# show
interfaces {
  so-3/0/0 {
    speed 100mb;
  }
}
[edit]
user@host# delete interfaces so-3/0/0 speed
[edit]
user@host# show
interfaces {
  so-3/0/0;
```

Copy a Statement in the Configuration

When you have many statements in a configuration that are similar, you can add one statement, then make copies of that statement. Copying a statement duplicates that statement and the entire hierarchy of statements configured under that statement. Copying statements is useful when you are configuring many physical or logical interfaces of the same type.

To make a copy of an existing statement in the configuration, use the configuration mode copy command:

```
copy existing-statement to new-statement
```

Immediately after you have copied a portion of the configuration, the configuration might not be valid. You must check the validity of the new configuration, and if necessary, modify either the copied portion or the original portion for the configuration to be valid.

Example: Copy a Statement in the Configuration

After you have created one virtual connection (VC) on an interface, copy its configuration to create a second VC:

```
[edit interfaces]
user@host# show
at-1/0/0 {
  description "PAIX to MAE West"
  encapsulation atm-pvc;
  unit 61 {
    point-to-point;
    vci 0.61;
    family inet {
      address 10.0.1.1/24;
    }
  }
}
```

```
[edit interfaces]
user@host# edit at-1/0/0
[edit interfaces at-1/0/0]
user@host# copy unit 61 to unit 62
[edit interfaces at-1/0/0]
user@host# show
description "PAIX to MAE West"
encapsulation atm-pvc;
  unit 61 {
    point-to-point;
    vci 0.61;
    family inet {
      address 10.0.1.1/24;
    }
  }
  unit 62 {
    point-to-point;
    vci 0.61;
    family inet {
      address 10.0.1.1/24;
    }
  }
}
```

Rename an Identifier

When modifying a configuration, you can rename an identifier that is already in the configuration. You can do this either by deleting the identifier (using the delete command) and then adding the renamed identifier (using the set and edit commands), or you can rename the identifier using the rename configuration mode command:

```
rename <statement-path> identifier1 to identifier2
```

Example: Rename an Identifier

Change the network time (NTP) server address to 10.0.0.6:

```
[edit]
user@host# rename system network-time server 10.0.0.7 to server 10.0.0.6
```

Insert a New Identifier

When configuring the router, you can enter most statements and identifiers in any order. Regardless of the order in which you enter the configuration statements, the CLI always displays the configuration in a strict order. However, there are a few cases where the ordering of the statements matters because the configuration statements create a sequence that is analyzed in order.

For example, in a routing policy or firewall filter, you define terms that are analyzed sequentially. Also, when you create a named path in dynamic Multiprotocol Label Switching (MPLS), you define an ordered list of the transit routers in the path, starting with the first transit router and ending with the last one.

To modify a portion of the configuration in which the statement order matters, use the insert configuration mode command:

```
insert <statement-path> identifier1 (before | after) identifier2
```

If you do not use the insert command, but instead simply configure the identifier, it is placed at the end of the list of similar identifiers.

Examples: Insert a New Identifier

Insert policy terms in a routing policy configuration. Note that if you do not use the insert command, but rather just configure another term, the added term is placed at the end of the existing list of terms.

```
[edit]
user@host# show
policy-options {
  policy-statement statics {
    term term1 {
      from {
        route-filter 192.168.0.0/16 orlonger;
        route-filter 224.0.0.0/3 orlonger;
      }
      then reject;
    }
    term term2 {
      from protocol direct;
      then reject;
    }
    term term3 {
      from protocol static;
      then reject;
    }
    term term4 {
      then accept;
    }
  }
}
[edit]
user@host# rename policy-options policy-statement statics term term4 to term term6
[edit]
user@host# set policy-options policy-statement statics term term4 from protocol local
[edit]
user@host# set policy-options policy-statement statics term term4 then reject
[edit]
user@host# set policy-options policy-statement statics term term5 from protocol aggregate
[edit]
user@host# set policy-options policy-statement statics term term5 then reject
[edit]
user@host# insert policy-options policy-statement statics term term4 after term term3
[edit]
user@host# insert policy-options policy-statement statics term term5 after term term4
[edit]
user@host# show policy-options policy-statement statics
```

```

term term1 {
  from {
    route-filter 192.168.0.0/16 orlonger;
    route-filter 224.0.0.0/3 orlonger;
  }
  then reject;
}
term term2 {    # reject direct routes
  from protocol direct;
  then reject;
}
term term3 {    # reject static routes
  from protocol static;
  then accept;
}
term term4 {    #reject local routes
  from protocol local;
  then reject;
}
term term5 {    #reject aggregate routes
  from protocol aggregate;
  then reject;
}
term term6 {    #accept all other routes
  then accept;
}

```

Insert a transit router in a dynamic MPLS path:

```

[edit protocols mpls path ny-sf]
user@host# show
1.1.1.1;
2.2.2.2;
3.3.3.3 loose;
4.4.4.4 strict;
6.6.6.6;
[edit protocols mpls path ny-sf]
user@host# insert 5.5.5.5 before 6.6.6.6
[edit protocols mpls path ny-sf]
user@host# set 5.5.5.5 strict
[edit protocols mpls path ny-sf]
user@host# show
1.1.1.1;
2.2.2.2;
3.3.3.3 loose;
4.4.4.4 strict;
5.5.5.5 strict;
6.6.6.6;

```

Run an Operational Mode CLI Command from Configuration Mode

At times, you might need to display the output of an operational mode show or other command while configuring the software. While in configuration mode, you can execute a single operational mode command by issuing the configuration mode run command and specifying the operational mode command:

```
[edit]
user@host# run operational-mode-command
```

Example: Run an Operational Mode CLI Command from Configuration Mode

Display the priority value of the VRRP master router while you are modifying the VRRP configuration for a backup router:

```
[edit interfaces ge-4/2/0 unit 0 family inet vrrp-group 27]
user@host# show
virtual-address [ 192.168.1.15 ];
[edit interfaces ge-4/2/0 unit 0 family inet vrrp-group 27]
user@host# run show vrrp detail
Physical interface: ge-5/2/0, Unit: 0, Address: 192.168.29.10/24
  Interface state: up, Group: 10, State: backup
  Priority: 190, Advertisement interval: 3, Authentication type: simple
  Preempt: yes, VIP count: 1, VIP: 192.168.29.55
  Dead timer: 8.326, Master priority: 201, Master router: 192.168.29.254
[edit interfaces ge-4/2/0 unit 0 family inet vrrp-group 27]
user@host# set priority ...
```

Display Configuration Mode Command History

In configuration mode, you can display a list of the recent commands you issued while in configuration mode. To do this, use the run show cli history command:

```
user@host> configure
...
[edit]
user@host# run show cli history
12:40:08 -- show
12:40:17 -- edit protocols
12:40:27 -- set isis
12:40:29 -- edit isis
12:40:40 -- run show cli history
[edit protocols isis]
user@host#
```

By default, this command displays the last 100 commands issued in the CLI. If you specify a number with the command, it displays that number of recent commands. For example:

```
user@host# run show cli history 3
12:40:08 -- show
12:40:17 -- edit protocols
12:40:27 -- set isis
```


Verify a Configuration

To verify that the syntax of a configuration is correct, use the configuration mode commit check command:

```
[edit]
user@host# commit check
configuration check succeeds
[edit]
user@host#
```

If the commit check command finds an error, a message indicates the location of the error.

Commit a Configuration

To save software configuration changes to the configuration database and activate the configuration on the router, use the commit configuration mode command:

```
[edit]
user@host# commit
commit complete
[edit]
user@host#
```

The configuration is checked for syntax errors. If the syntax is correct, the configuration is activated and becomes the current, operational router configuration.

You can issue the commit command from any hierarchy level.

There are two ways to commit configurations:

- Commit a Configuration and Exit Configuration Mode on page 158
- Activate a Configuration but Require Confirmation on page 158

If the configuration contains syntax errors, a message indicates the location of the error and the configuration is not activated. The error message has the following format:

```
[edit edit-path]
'offending-statement;'
error-message
```

For example:

```
[edit firewall filter login-allowed term allowed from]
'icmp-type [ echo-request echo-reply ];'
keyword 'echo-reply' unrecognized
```

You must correct the error before recommitting the configuration. To return quickly to the hierarchy level where the error is located, copy the path from the first line of the error and paste it at the configuration mode prompt at the [edit] hierarchy level.

When you commit a configuration, you commit the entire configuration in its current form. If more than one user is modifying the configuration, committing it saves and activates the changes of all the users.

After you commit the configuration and are satisfied that it is running successfully, you should issue the request system snapshot command to back up the new software onto the /altconfig file system. If you do not issue the request system snapshot command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The request system snapshot command backs up the root file system to /altroot, and /config to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.



After you issue this command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Note

Commit a Configuration and Exit Configuration Mode

To save software configuration changes, activate the configuration on the router, and exit configuration mode, use the commit and-quit configuration mode command. This command succeeds only if the configuration contains no errors.

```
[edit]
user@host# commit and-quit
commit complete
exiting configuration mode
user@host>
```

Activate a Configuration but Require Confirmation

You can commit the current candidate configuration but require an explicit confirmation for the commit to become permanent. This is useful for verifying that a configuration change works correctly and does not prevent management access to the router. If the change prevents access or causes other errors, the automatic rollback to the previous configuration restores access after the rollback confirmation timeout passes.

To commit the current candidate configuration but require an explicit confirmation for the commit to become permanent, use the commit confirmed configuration mode command:

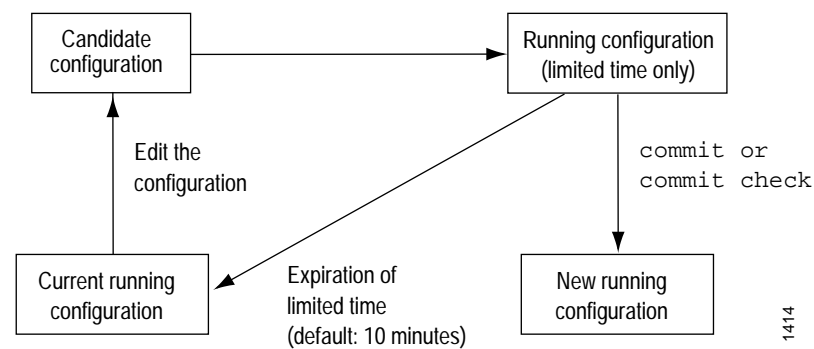
```
[edit]
user@host# commit confirmed
commit complete
[edit]
user@host#
```

To keep the new configuration active, enter a `commit` or `commit check` command within 10 minutes of the `commit confirmed` command. If the `commit` is not confirmed within a certain amount of time (10 minutes by default), the JUNOS software automatically rolls back to the previous configuration.

Like the `commit` command, the `commit confirmed` command verifies the configuration syntax and reports any errors. If there are no errors, the configuration is activated and begins running on the router.

Figure 5 illustrates how the `commit confirmed` command works.

Figure 5: Confirm a Configuration



To change the amount of time before you have to confirm the new configuration, specify the number of minutes when you issue the command:

```

[edit]
user@host# commit confirmed minutes
commit complete
[edit]
user@host#
  
```

Synchronize Routing Engines

If your router has two Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the other by issuing the `commit synchronize` command. The Routing Engine on which you execute this command (requesting Routing Engine) copies and loads its candidate configuration to the other (responding Routing Engine). Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

For example, if you are logged in to `re1` (requesting Routing Engine) and you want `re0` (responding Routing Engine) to have the same configuration as `re1`, issue the `commit synchronize` command on `re1`. `re1` copies and loads its candidate configuration to `re0`. Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, `re1`'s candidate configuration is activated and becomes the current operational configuration on both Routing Engines.



Note

When you issue the `commit synchronize` command, you must use the `apply groups re0` and `re1`. For information about how to use the `apply groups` statement, see “Apply a Configuration Group” on page 181.

The responding Routing Engine must use JUNOS release 5.0 or higher.

To synchronize a Routing Engine's current operational configuration file with the other, log in to the Routing Engine from which you want to synchronize and issue the `commit synchronize` command:

```
[edit]
user@host# commit synchronize
commit complete
[edit]
user@host#
```

Example: Apply Groups `re0` and `re1`

The following example shows `apply groups re0` and `re1` with some configuration data that might be different on `re0` and `re1`.

```
re0 {
  system {
    host-name my_router_RE0;
  }
  interfaces {
    fxp0 {
      unit 0 {
        family inet {
          address 192.168.15.49/24;
        }
        family iso;
      }
    }
  }
}
```

```

re1 {
  system {
    host-name my_router_RE1;
  }
  interfaces {
    fxp0 {
      unit 0 {
        family inet {
          address 192.168.15.50/24;
        }
        family iso;
      }
    }
  }
}

```

Example: Set Apply Groups Re0 and Re1

The following example sets the apply groups re0 and re1:

```

[edit]
user@host# set apply-groups [re0 re1]
[edit]
user@host#

```

Save a Configuration to a File

You might want to save the configuration to a file so that you can edit it with a text editor of your choice. You can save your current configuration to an ASCII file, which saves the configuration in its current form, including any uncommitted changes. If more than one user is modifying the configuration, all changes made by all users are saved.

To save software configuration changes to an ASCII file, use the save configuration mode command:

```

[edit]
user@host# save filename
[edit]
user@host#

```

By default, the configuration is saved to a file in your home directory, which is on the flash disk. For information about specifying the filename, see “How to Specify Filenames and URLs” on page 224.

Load a Configuration

You can create a file, copy the file to the local router, and then load the file into the CLI. After you have loaded the file, you can commit it to activate the configuration on the router, or you can edit the configuration interactively using the CLI and commit it at a later time.

You can also create a configuration while typing at the terminal and then load it. Loading a configuration from the terminal is generally useful when you are cutting existing portions of the configuration and pasting them elsewhere in the configuration.

To load an existing configuration file that is located on the router, use the load configuration mode command:

```
[edit]
user@host# load (replace | merge | override) filename
```

To load a configuration from the terminal, use the following version of the load configuration mode command:

```
[edit]
user@host# load (replace | merge | override) terminal
[Type ^D to end input]
```

To replace an entire configuration, specify the override option. An override operation discards the current candidate configuration and loads the configuration in *filename* or the one that you type at the terminal.

To combine the current configuration and the configuration in *filename* or the one that you type at the terminal, specify the merge option. A merge operation is useful when you are adding a new section to an existing configuration. If the existing configuration and the incoming configuration contain conflicting statements, the statements in the incoming configuration override those in the existing configuration.

To replace portions of a configuration, specify the replace option. For this operation to work, you must include `replace: tags` in the file or configuration you type at the terminal. The software searches for the `replace: tags`, deletes the existing statements of the same name, if any, and replaces them with the incoming configuration. If there is no existing statement of the same name, the replace operation adds to the configuration the statements marked with `replace: tag`.

If, in an override or merge operation, you specify a file or type text that contains `replace: tags`, the `replace: tags` are ignored, and the override or merge operation is performed.

If you are performing a replace operation and the file you specify or text you type does not contain any `replace: tags`, the replace operation is effectively equivalent to a merge operation. This might be useful if you are running automated scripts and cannot know in advance whether the scripts need to perform a replace or a merge operation. The scripts can use the replace operation to cover either case.

For information about specifying the filename, see “How to Specify Filenames and URLs” on page 224.

To copy a configuration file from another network system to the local router, you can use the ssh and Telnet utilities, as described in the *JUNOS Internet Software Operational Mode Command Reference*.

Examples: Load a Configuration from a File

Figure 6: Example 1: Load a Configuration from a File

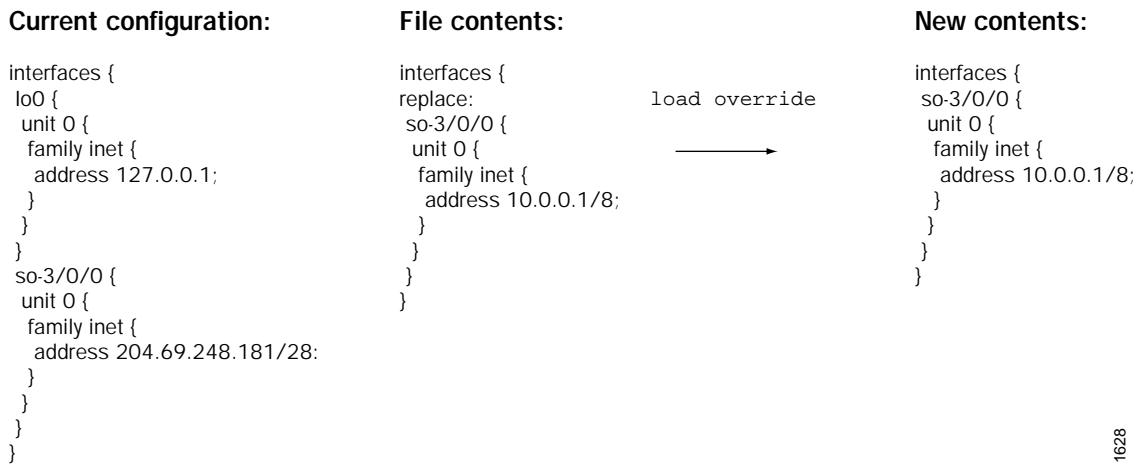


Figure 7: Example 2: Load a Configuration from a File

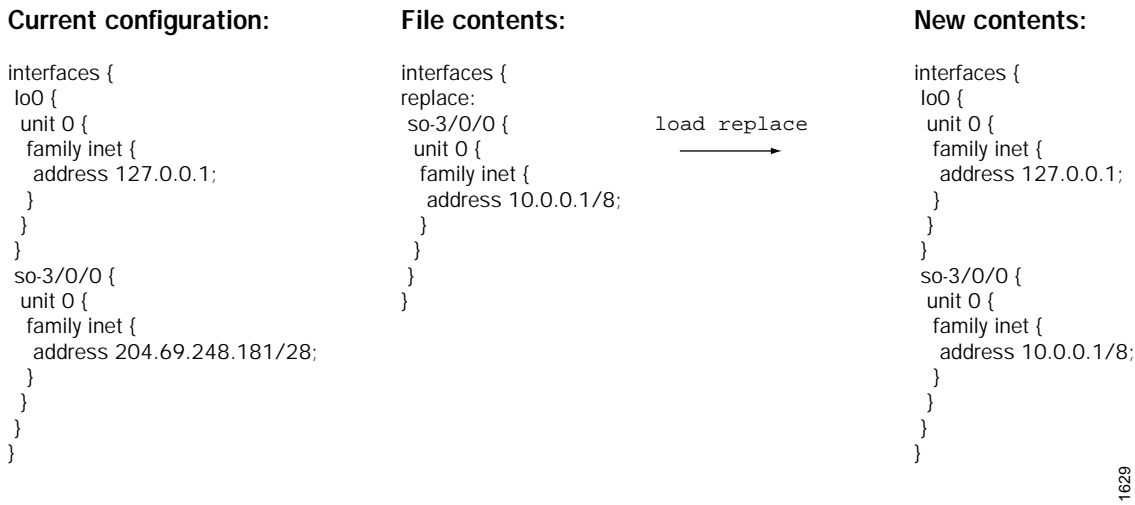
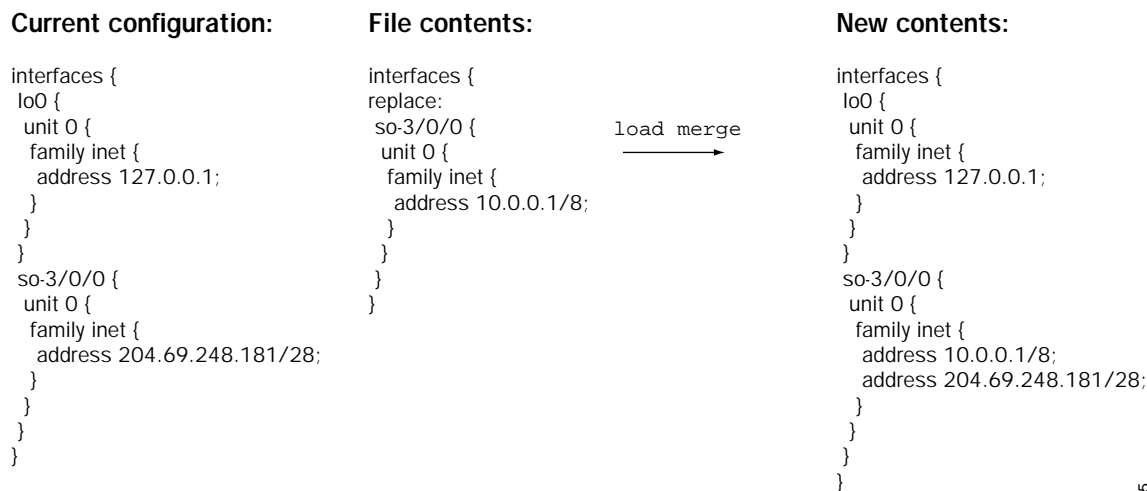


Figure 8: Example 3: Load a Configuration from a File



1705

Return to a Previously Committed Configuration

To return to the most recently committed configuration and load it into configuration mode without activating it, use the rollback configuration mode command:

```

[edit]
user@host# rollback
load complete

```

To activate the configuration that you loaded, use the commit command:

```

[edit]
user@host# rollback
load complete
[edit]
user@host# commit

```

To return to a configuration prior to the most recently committed one, include the number in the rollback command:

```

[edit]
user@host# rollback number
load complete

```

number can be a number in the range 0 through 9. The most recently saved configuration is number 0 (which is the default configuration to which the system returns), and the oldest saved configuration is number 9.

To display previous configurations, including rollback number, date, time, the name of the user who committed changes, and the method of commit, use the rollback ? command.

```
[edit]
user@host# rollback ?
Possible completions:
<[Enter]> Execute this command
<number> Numeric argument
0 2001-02-27 12:52:10 PST by abc via cli
1 2001-02-26 14:47:42 PST by cde via cli
2 2001-02-14 21:55:45 PST by fgh via cli
3 2001-02-10 16:11:30 PST by hij via cli
4 2001-02-10 16:02:35 PST by klm via cli
| Pipe through a command
[edit]
```

For more information about configuration versions, see “How the Configuration Is Stored” on page 130.

The access privilege level for using the rollback command is controlled by the rollback permission bit. Users for whom this permission bit is not set can return only to the most recently committed configuration. Users for whom this bit is set can return to any prior committed configuration. For more information, see “Configure Access Privilege Levels” on page 254.

Example: Return to a Previously Committed Version of the Configuration

Return to and activate the version stored in the file juniper.conf.3:

```
[edit]
user@host# rollback 3
load complete
[edit]
user@host# commit
```

Configuration Mode Error Messages

If you do not type an option for a statement that requires one, a message indicates the type of information expected.

In this example, you need to type an area number to complete the command:

```
[edit]
user@host# set protocols ospf area<Enter>
                                     ^
syntax error, expecting <identifier>.
```

In this example, you need to type a value for the hello interval to complete the command:

```
[edit]
user@host# set protocols ospf area 45 interface so-0/0/0
             hello-interval<Enter>
                               ^
syntax error, expecting <data>
```

If you have omitted a required statement at a particular hierarchy level, when you attempt to move from that hierarchy level or when you issue the show command in configuration mode, a message indicates which statement is missing. For example:

```
[edit protocols pim interface so-0/0/0]
user@host# top
Warning: missing mandatory statement: 'mode'
[edit]
user@host# show
protocols {
  pim {
    interface so-0/0/0 {
      priority 4;
      version 2;
      # Warning: missing mandatory statement(s): 'mode'
    }
  }
}
```

Deactivate and Reactivate Statements and Identifiers in a Configuration

In a configuration, you can deactivate statements and identifiers so that they do not take effect when you issue the commit command. Any deactivated statements and identifiers are marked with the inactive: tag. They remain in the configuration, but are not activated when you issue a commit command.

To deactivate a statement or identifier, use the deactivate configuration mode command:

```
deactivate (statement | identifier)
```

To reactivate a statement or identifier, use the activate configuration mode command:

```
activate (statement | identifier)
```

In both commands, the *statement* or *identifier* you specify must be at the current hierarchy level.

In some portions of the configuration hierarchy, you can include a disable statement to disable functionality. One example is disabling an interface by including the disable statement at the [edit interface *interface-name*] hierarchy level. When you deactivate a statement, that specific object or property is completely ignored and is not applied at all when you issue a commit command. When you disable a functionality, it is activated when you issue a commit command but is treated as though it is down or administratively disabled.

Examples: Deactivate and Reactivate Statements and Identifiers in a Configuration

Deactivate an interface in the configuration:

```
[edit interfaces]
user@host# show
at-5/2/0 {
  traceoptions {
    traceflag all;
  }
  atm-options {
    vpi 0 maximum-vcs 256;
  }
  unit 0 {
  ...
[edit interfaces]
user@host# deactivate at-5/2/0
[edit interfaces]
user@host# show
inactive: at-5/2/0 {
  traceoptions {
    traceflag all;
  }
  ...
```

Reactivate the interface:

```
[edit interfaces]
user@host# activate at-5/2/0
[edit interfaces]
user@host# show
at-5/2/0 {
  traceoptions {
    traceflag all;
  }
  ...
```

Add Comments in a Configuration

You can include comments in a configuration to describe any statement in the configuration. You can add commands interactively in the CLI and by editing the ASCII configuration file.

When you add comments in configuration mode, they are associated with a statement at the current level. Each statement can have one single-line comment associated with it. Before you can associate a comment with a statement, the statement must exist. The comment is placed on the line preceding the statement.

To add comments to a configuration, use the `annotate configuration mode` command:

```
annotate statement "comment-string"
```

statement is the configuration statement to which you are attaching the comment; it must be at the current hierarchy level. If a comment for the specified *statement* already exists, it is deleted and replaced with the new comment.

comment-string is the text of the comment. The comment text can be any length, and you must type it on a single line. If the comment contains spaces, you must enclose it in quotation marks. In the comment string, you can include the comment delimiters `/* */` or `#`. If you do not specify any, the comment string is enclosed with the `/* */` comment delimiters.

To delete an existing comment, specify an empty comment string:

```
annotate statement ""
```

When you edit the ASCII configuration file and add comments, they can be one or more lines and must precede the statement they are associated with. If you place the comments in other places in the file, such as on the same line following a statement or on a separate line following a statement, they are removed when you use the load command to open the configuration into the CLI.

When you include comments in the configuration file directly, you can format comments in the following ways:

- Start the comment with a `/*` and end it with a `*/`. The comment text can be on a single line or can span multiple lines.
- Start the comment with a `#` and end it with a new line (carriage return).

If you add comments with the annotate command, you can view the comments within the configuration by entering the show configuration mode command or the show configuration operational mode command.

When configuring interfaces, you can add comments about the interface by including the description statement at the [edit interfaces *interface-name*] hierarchy level. Any comments you include appear in the output of the show interfaces commands. For more information about the description statement, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Examples: Include Comments in Configurations

Add comments to a configuration:

```
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host# set area 0.0.0.0
user@host# annotate area 0.0.0.0 "Backbone area configuration added June 15, 1998"
[edit protocols ospf]
user@host# edit area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# annotate interface so0 "Interface from router sj1 to router sj2"
```

```
[edit protocols ospf area 0.0.0.0]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    /* Backbone area configuration added June 15, 1998 */
    area 0.0.0.0 {
      /* Interface from router sj1 to router sj2 */
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
[edit]
user@host#
```

The following excerpt from a configuration example illustrates how to enter comments in a configuration file:

```
/* This comment goes with routing-options */
routing-options {
  /* This comment goes with routing-options traceoptions */
  traceoptions {
    /* This comment goes with routing-options traceoptions tracefile */
    tracefile rpd size 1m files 10;
    /* This comment goes with routing-options traceoptions traceflag task */
    traceflag task;
    /* This comment goes with routing-options traceoptions traceflag general */
    traceflag general;
  }
  autonomous-system 10458; /* This comment is dropped */
}
routing-options {
  rib-groups {
    ifrg {
      import-rib [ inet.0 inet.2 ];
      /* A comment here is dropped */
    }
    dvmrp-rib {
      import-rib inet.2;
      export-rib inet.2;
      /* A comment here is dropped */
    }
    /* A comment here is dropped */
  }
}
/* A comment here is dropped */
}
```

Have Multiple Users Configure the Software

Up to 32 users can be in configuration mode simultaneously, and they all can be making changes to the configuration. All changes made by all users are visible to everyone editing the configuration—the changes become visible as soon as the user presses the Enter key at the end of a command that changes the configuration, such as set, edit, or delete.

When any of the users editing the configuration issues a commit command, all changes made by all users are checked and activated.

Example: Using the CLI to Configure the Router

This section walks through an example of creating a simple configuration, illustrating how to use the CLI to create, display, and modify the software configuration for your system. The example used in this section creates the following configuration:

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
      }
    }
  }
}
```

Shortcut

You can create this entire configuration with two commands:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5 dead-interval 20
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/1 hello-interval 5 dead-interval 20
```

Longer Configuration Example

The remainder of this section provides a longer example of creating the OSPF configuration. In the process, it illustrates how to use the different features of the CLI.

First, you enter configuration mode by issuing the configure top-level command:

```
user@host> configure
entering configuration mode
[edit]
user@host#
```

The prompt in braces shows that you are in configuration edit mode, at the top of the hierarchy. If you want to create the above configuration, you start by editing the protocols ospf statements:

```
[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host#
```

Now, add the OSPF area:

```
[edit protocols ospf]
user@host# edit area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host#
```

Next, add the first interface:

```
[edit protocols ospf area 0.0.0.0]
user@host# edit interface so0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host#
```

You now have four nested statements. Next, set the hello and dead intervals. Note that command completion (enter a tab or space) and context-sensitive help (type a question mark) are always available.

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
> authentication-key    Authentication key
  dead-interval         Dead interval (seconds)
  disable               Disable OSPF on this interface
  hello-interval        Hello interval (seconds)
  interface-type        Type of interface
  metric                Interface metric (1..65535)
> neighbor              NBMA neighbor
  passive              Do not run OSPF, but advertise it
  poll-interval         Poll interval for NBMA interfaces
  priority              Designated router priority
  retransmit-interval   Retransmission interval (seconds)
  transit-delay         Transit delay (seconds)
  transmit-interval     OSPF packet transmit interval (milliseconds)
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set hello-interval 5
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set dead-interval 20
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host#
```

You can see what is configured at the current level with the show command:

```
[edit protocols ospf area 0.0.0.0 interface so-0]
user@host# show
hello-interval 5;
dead-interval 20;
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host#
```

You are finished at this level, so back up a level and take a look at what you have so far:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# up
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
    hello-interval 5;
    dead-interval 20;
}
[edit protocols ospf area 0.0.0.0]
user@host#
```

The interface statement appears because you have moved to the area statement.

Now, add the second interface:

```
[edit protocols ospf area 0.0.0.0]
user@host# edit interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set hello-interval 5
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set dead-interval 20
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# up
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
    hello-interval 5;
    dead-interval 20;
}
interface so-0/0/1 {
    hello-interval 5;
    dead-interval 20;
}
[edit protocols ospf area 0.0.0.0]
user@host#
```

Now, back up to the top level and see what you have:

```
[edit protocols ospf area 0.0.0.0]
user@host# top
[edit]
user@host# show
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0 {
                hello-interval 5;
                dead-interval 20;
            }
            interface so-0/0/1 {
                hello-interval 5;
                dead-interval 20;
            }
        }
    }
}
[edit]
user@host#
```


This configuration now contains the statements you want. Before committing it, which activates the configuration, verify that the configuration is correct:

```
[edit]
user@host# commit check
configuration check succeeds
[edit]
user@host#
```

Now you can commit the configuration to activate it on the router:

```
[edit]
user@host# commit
commit complete
[edit]
user@host#
```

Suppose you decide to use different dead and hello intervals on interface so-0/0/1. You can make changes to the configuration. You can go directly to the appropriate hierarchy level by typing the full hierarchy path to the statement you want to edit.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# show
hello-interval 5;
dead-interval 20;
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set hello-interval 7
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set dead-interval 28
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {
        hello-interval 7;
        dead-interval 28;
      }
    }
  }
}
[edit]
user@host#
```

If you change your mind and decide not to run OSPF on the first interface, you can delete the statement:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# delete interface so-0/0/0
[edit protocols ospf area 0.0.0.0]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1 {
        hello-interval 7;
        dead-interval 28;
      }
    }
  }
}
[edit]
user@host#
```

Note that everything inside of the statement you deleted was deleted with it. You could eliminate the entire OSPF configuration by simply entering `delete protocols ospf` while at the top level.

Suppose you decide to use the default values for the hello and dead intervals on your remaining interface, but you want OSPF to run on that interface:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# delete hello-interval
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# delete dead-interval
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1;
    }
  }
}
[edit]
user@host#
```

You can set multiple statements at the same time as long as they are all part of the same hierarchy (the path of statements from the top inward, as well as one or more statements at the bottom of the hierarchy). Doing this can reduce considerably the number of commands you must enter. For example, if you want to go back to the original hello and dead interval timers on interface so-0/0/1, you can enter:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set hello-interval 5 dead-interval 20
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# exit
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
      }
    }
  }
}
[edit]
user@host#
```

You also can re-create the other interface, as you had it before, with only a single entry:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/1 hello-interval 5 dead-interval 20
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
      }
    }
  }
}
}
```

Additional Details about Specifying Statements and Identifiers

This section provides more detailed information about specifying statements and identifiers in configuration mode:

- How to Specify Statements on page 176
- How the CLI Performs Type-Checking on page 178

How to Specify Statements

This section provides more detailed information about CLI container and leaf statements so that you can better understand how the CLI displays them in a configuration and how you must specify them when creating ASCII configuration files.

Statements are shown one of two ways, either with braces or without:

- Statement name and identifier, with one or more lower-level statements enclosed in braces:

```
< statement-name > < identifier > {
    statement;
    additional-statements;
}
```

- Statement name, identifier, and a single identifier:

```
< statement-name > < identifier > identifier;
```

The *statement-name* is the name of the statement. In the configuration example shown in the previous section, *ospf* and *area* are statement names.

The *identifier* is a name or other string that uniquely identifies an instance of a statement. The identifier is used when a statement can be specified more than once in a configuration. In the configuration example shown in the previous section, the identifier for the *area* statement is *0* and the identifier for the *interface* statement is *so-0/0/0*.

When specifying a statement, you must specify either a statement name or an identifier, or both, depending on the statement hierarchy.

You specify identifiers in one of the following ways:

- *identifier*—The *identifier* is a flag, which is a single keyword.
- *identifier value*—The *identifier* is a keyword, and the *value* is a required option variable.
- *identifier [value1 value 2 value3 ...]*—The *identifier* is a set that accepts multiple values. The brackets are required when you specify a set of identifiers; however, they are optional when you specify only one identifier.

The following examples illustrate how statements and identifiers are specified in the configuration:

```

protocol {                # Top-level statement (statement-name).
  ospf {                  # Statement under "protocol" (statement-name).
    area 0.0.0.0 {        # OSPF area "0.0.0.0" (statement-name identifier),
      interface so-0/0/0 { # which contains an interface named "so-0/0/0."
        hello-interval 25; # Identifier and value (identifier-name value).
        priority 2;        # Identifier and value (identifier-name value).
        disable;          # Flag identifier (identifier-name).
      }
      interface so-0/0/1; # Another instance of "interface," named so-0/0/1,
    }                    # this instance contains no data, so no braces
  }                      # are displayed.
}
policy-options {          # Top-level statement (statement-name).
  term term1 {            # Statement under "policy-options"
    from {                # (statement-name value).
      route-filter 10.0.0.0/8 orlonger reject; # Statement under "term" (statement-name).
      route-filter 127.0.0.0/8 orlonger reject; # One identifier ("route-filter") with
      route-filter 128.0.0.0/16 orlonger reject; # multiple values.
      route-filter 149.20.64.0/24 orlonger reject;
      route-filter 172.16.0.0/12 orlonger reject;
      route-filter 191.255.0.0/16 orlonger reject;
    }
    then {                # Statement under "term" (statement-name).
      next term;          # Identifier (identifier-name).
    }
  }
}

```

When you create an ASCII configuration file, you can specify statements and identifiers in one of the following ways. However, each statement has a preferred style, and the CLI uses that style when displaying the configuration in response to a configuration mode show command.

■ Statement followed by identifiers:

```
statement-name identifier-name [...] identifier-name value [...];
```

■ Statement followed by identifiers enclosed in braces:

```
statement-name {
  identifier-name;
  [...]
  identifier-name value;
  [...]
}
```

■ For some repeating identifiers, you can use one set of braces for all the statements:

```
statement-name {
  identifier-name value1;
  identifier-name value2;
}
```

How the CLI Performs Type-Checking

When you specify identifiers and values, the CLI expects to receive specific types of input and performs type-checking to verify that the data you entered is in the correct format. For example, for a statement in which you must specify an IP address, the CLI checks that you entered an address in a valid format. If you have not, an error message indicates what you were expected to type. Table 7 lists the data types the CLI checks.

Table 7: CLI Configuration Input Types

Data Type	Format	Examples
Physical interface name (used in the edit interfaces hierarchy)	<i>type-fpc/pic/port</i>	Correct: so-0/0/1 Incorrect: so-0
Full interface name	<i>type-fpc/pic/port<:channel>.logical</i>	Correct: so-0/0/1.0 Incorrect: so-0/0/1
Full or abbreviated interface name (used in places other than the edit interfaces hierarchy)	<i>type-<fpc/>pic/port>><:channel>.logical></i>	Correct: so, so-1, so-1/2/3:4.5
IP address	<i>0xhex-bytes</i> <i>octet<.octet<.octet.<octet>>></i>	Correct: 1.2.3.4, 0x01020304, 128.8.1, 128.8 Sample translations: 1.2.3 becomes 1.2.3.0 0x01020304 becomes 1.2.3.4 0x010203 becomes 0.1.2.3
IP address (destination prefix) and prefix length	<i>0xhex-bytes</length></i> <i>octet<.octet<.octet.<octet>>></length></i>	Correct: 10/8, 128.8/16, 1.2.3.4/32, 1.2.3.4 Sample translations: 1.2.3 becomes 1.2.3.0/32 0x01020304 becomes 1.2.3.4/32 0x010203 becomes 0.1.2.3/32 default becomes 0.0.0.0/0
ISO address	<i>hex-nibble<hex-nibble ...></i>	Correct: 47.1234.2345.3456.00, 47123423453456.00, 47.12.34.23.45.34.56.00 Sample translations: 47123456 becomes 47.1234.56 47.12.34.56 becomes 47.1234.56 4712.3456 becomes 47.1234.56
OSPF area identifier (ID)	<i>0xhex-bytes</i> <i>octet<.octet<.octet.<octet>>></i> <i>decimal-number</i>	Correct: 54, 0.0.0.54, 0x01020304, 1.2.3.4 Sample translations: 54 becomes 0.0.0.54 257 becomes 0.0.1.1 128.8 becomes 128.8.0.0 0x010203 becomes 0.1.2.3

Chapter 13

Configuration Groups

This chapter discusses the following topics:

- Overview on page 179
- Configuration Groups Configuration Statements on page 180
- Configuration Groups Configuration Guidelines on page 180
- Examples: Configuration Groups on page 187
- Summary of Configuration Group Statements on page 195

Overview

Configuration groups allow you to create a group containing configuration statements and to direct the inheritance of that group's statements in the rest of the configuration. The same group can be applied to different sections of the configuration, and different sections of one group's configuration statements can be inherited in different places in the configuration.

Configuration groups allow you to create smaller, more logically constructed configuration files, making it easier to configure and maintain the JUNOS software. For example, you can group statements that are repeated in many places in the configuration, such as when configuring interfaces, and thereby limit updates to just the group.

You can also use wildcards in a configuration group to allow configuration data to be inherited by any object that matches a wildcard expression.

The configuration group mechanism is separate from the grouping mechanisms used elsewhere in the configuration, such as BGP groups. Configuration groups provide a generic mechanism that can be used throughout the configuration but that are known only to the JUNOS CLI. The individual software processes that perform the actions directed by the configuration receive the expanded form of the configuration; they have no knowledge of configuration groups.

Inheritance Model

Configuration groups use true inheritance, which involves a dynamic, ongoing relationship between the source of the configuration data and the target of that data. Data values changed in the configuration group are automatically inherited by the target. The target need not contain the inherited information, although the inherited values can be overridden in the target without affecting the source from which they were inherited.

This inheritance model allows you to see only the instance-specific information without seeing the inherited details. A command pipe in configuration mode allows you to display the inherited data.

Configuration Groups Configuration Statements

To configure configuration groups and inheritance, you can include the following statements in the configuration:

```
groups {
  group-name {
    configuration-data;
  }
}
```

Include the `apply-groups [group-names]` statement anywhere in the configuration that the configuration statements contained in a configuration group are needed.

Configuration Groups Configuration Guidelines

For areas of your configuration to inherit configuration statements, you must first put the statements into a configuration group and then apply that group to the levels in the configuration hierarchy that require the statements. This section covers the following topics:

- Create a Configuration Group on page 181
- Apply a Configuration Group on page 181
- Display Inherited Values on page 183
- Use Wildcards on page 184

Create a Configuration Group

To create a configuration group, include the groups statement at the [edit] hierarchy level:

```
groups {
  group-name {
    configuration-data;
  }
}
```

group-name is the name of a configuration group. To configure multiple groups, specify more than one *group-name*. On routers that support multiple Routing Engines, you can also specify two special group names:

- re0—Configuration statements applied to the Routing Engine in slot 0.
- re1—Configuration statements applied to the Routing Engine in slot 1.

The configuration specified in group re0 is only applied if the current Routing Engine is in slot 0; likewise, the configuration specified in group re1 is only applied if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each re0 or re1 group contains at a minimum the configuration for the hostname and the management interface (fxp0). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

configuration-data contains the configuration statements applied elsewhere in the configuration with the apply-groups statement, to have the target configuration inherit the statements in the group.

Apply a Configuration Group

To have a configuration inherit the statements in a configuration group, include the apply-groups statement:

```
apply-groups [ group-name ];
```

If you specify more than one group name, list them in order of inheritance priority. The configuration data in the first group takes priority over the data in subsequent groups.

For routers that support multiple Routing Engines, you can specify re0 and re1 as group names. The configuration specified in group re0 is only applied if the current Routing Engine is in slot 0; likewise, the configuration specified in group re1 is only applied if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each re0 or re1 group contains at a minimum the configuration for the hostname and the management interface (fxp0). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

You can include the apply-groups statement at any level of the configuration hierarchy, listing group names within each apply-groups statement in priority order.

You can include only one `apply-groups` statement at each specific level of the configuration hierarchy. The `apply-groups` statement at a specific hierarchy level lists the configuration groups to be added to the containing statement's list of configuration groups.

Values specified at the specific hierarchy level override values inherited from the configuration group.

Groups listed in nested `apply-groups` statements take priority over groups in outer statements. In the following example, the BGP neighbor 10.0.0.1 inherits configuration data from group one first, then from groups two and three. Configuration data in group one overrides data in any other group. Data from group ten is used only if a statement is not contained in any other group.

```

apply-groups [ eight nine ten ];
protocols {
  apply-groups seven;
  bgp {
    apply-groups [ five six ];
    group some-bgp-group {
      apply-groups four;
      neighbor 10.0.0.1 {
        apply-groups [ one two three ];
      }
    }
  }
}

```

Example: Configure and Apply Configuration Groups

In this example, the SNMP configuration is divided between the group `basic` and the normal configuration hierarchy.

There are a number of advantages to placing the system-specific configuration (SNMP contact) into a configuration group and thus separating it from the normal configuration hierarchy—the user can replace (using the `load replace` command) either section without discarding data from the other.

In addition, setting a contact for a specific box is now possible because the group data would be hidden by the router-specific data.

```

[edit]
groups {
  basic {
    # "groups" is a top-level statement
    # User defined group name
    snmp {
      # This group contains some snmp data
      contact "My Engineering Group";
      community BasicAccess {
        authorization read-only;
      }
    }
  }
}
apply-groups basic; # Enable inheritance from group "basic"
snmp {
  # Some normal (non-group) configuration
  location "West of Nowhere";
}

```

This configuration is equivalent to the following:

```
[edit]
snmp {
  location "West of Nowhere";
  contact "My Engineering Group";
  community BasicAccess {
    authorization read-only;
  }
}
```

Display Inherited Values

Configuration groups can add some confusion regarding the actual values used by the router, because configuration data can be inherited from configuration groups. To view the actual values used by the router, use the display inheritance command after the pipe in a show command. This command displays the inherited statements at the level at which they are inherited and the group from which they have been inherited.

```
[edit]
user@host# show | display inheritance
snmp {
  location "West of Nowhere";
  ##
  ## 'My Engineering Group' was inherited from group 'basic'
  ##
  contact "My Engineering Group";
  ##
  ## 'BasicAccess' was inherited from group 'basic'
  ##
  community BasicAccess {
    ##
    ## 'read-only' was inherited from group 'basic'
    ##
    authorization read-only;
  }
}
```

To display the expanded configuration (the configuration, including the inherited statements) without the ## lines, use the except command after the pipe in a show command:

```
[edit]
user@host# show | display inheritance | except ##
snmp {
  location "West of Nowhere";
  contact "My Engineering Group";
  community BasicAccess {
    authorization read-only;
  }
}
```

Use Wildcards

You can use wildcards to identify names and allow one statement to provide data for a variety of statements. For example, grouping the configuration of the sonet-options statement over all SONET/SDH interfaces or the dead interval for OSPF over all ATM interfaces simplifies configuration files and eases their maintenance.

Wildcarding in normal configuration data is done in a style that is consistent with traditional UNIX shell name wildcarding. In this style of wildcarding, you can use the following metacharacters:

- Asterisk (*)—Matches any string of characters.
- Question mark (?)—Matches any single character.
- Open bracket ([)—Introduces a character class.
- Close bracket (])—Indicates the end of a character class. If the close bracket is missing, the open bracket matches a [rather than introduces a character class.
- A character class matches any of the characters between the square brackets. Character classes must be enclosed in quotation marks (" ").
- Hyphen (-)—Specifies a range of characters.
- Exclamation point (!)—The character class can be complemented by making an exclamation point the first character of the character class. To include a] in a character class, make it the first character listed (after the !, if any). To include a minus sign, make it the first or last character listed.

Wildcarding in configuration groups follows the same rules, but the wildcard pattern must be enclosed in angle brackets (<pattern>) to differentiate it from other wildcarding in the configuration file. For example:

```
[edit]
groups {
  sonet-default {
    interfaces {
      <so-*> {
        sonet-options {
          payload-scrambler;
          rfc-2615;
        }
      }
    }
  }
}
```

Wildcard expressions match (and provide configuration data for) existing statements in the configuration that match their expression only. In the example above, the expression <so-*> passes its sonet-options statement to any interface that matches the expression so-*.

Angle brackets allow you to pass normal wildcarding through without modification. In all matching within the configuration, whether it is done with or without wildcards, the first item encountered in the configuration that matches is used. In the following example, data from the wildcarded BGP groups is inherited in the order in which the groups are listed. The preference value from <*a*> overrides the preference in <*b*>, just as the p value from <*c*> overrides the one from <*d*>. Data values from any of these groups override the data values from abcd.

```
[edit]
user@host# show
groups {
  one {
    protocols {
      bgp {
        group <*a*> {
          preference 1;
        }
        group <*b*> {
          preference 2;
        }
        group <*c*> {
          out-delay 3;
        }
        group <*d*> {
          out-delay 4;
        }
        group abcd {
          preference 10;
          hold-time 10;
          out-delay 10;
        }
      }
    }
  }
}
protocols {
  bgp {
    group abcd {
      apply-groups one;
    }
  }
}
[edit]
user@host# show | display inheritance
protocols {
  bgp {
    group abcd {
      ##
      ## '1' was inherited from group 'one'
      ##
      preference 1;
      ##
      ## '10' was inherited from group 'one'
      ##
      hold-time 10;
      ##
      ## '3' was inherited from group 'one'
      ##
      out-delay 3;
    }
  }
}
```

Example: Use Wildcards

The following example demonstrates the use of wildcarding. The interface so-0/0/0 inherits data from the various SONET/SDH interface wildcard patterns in group one.

```
[edit]
user@host# show
groups {
  one {
    interfaces {
      <so-*> {
        sonet-options {
          rfc-2615;
        }
      }
      <so-0/*> {
        sonet-options {
          fcs 32;
        }
      }
      <so-*0/*> {
        sonet-options {
          fcs 16;
        }
      }
      <so-*/*0> {
        sonet-options {
          payload-scrambler;
        }
      }
    }
  }
}
apply-groups one;
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        address 10.0.0.1/8;
      }
    }
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  so-0/0/0 {
    ##
    ## 'sonet-options' was inherited from group 'one'
    ##
    sonet-options {
      ##
      ## '32' was inherited from group 'one'
      ##
      fcs 32;
      ##
      ## 'payload-scrambler' was inherited from group 'one'
      ##
    }
  }
}
```

```

        payload-scrambler;
        ##
        ## 'rfc-2615' was inherited from group 'one'
        ##
        rfc-2615;
    }
    unit 0 {
        family inet {
            address 10.0.0.1/8;
        }
    }
}

```

Examples: Configuration Groups

The following examples illustrate ways to use configuration groups and inheritance:

- Configure Sets of Statements on page 187
- Configure Interfaces on page 189
- Configure Peer Entities on page 191
- Establish Regional Configurations on page 193
- Select Wildcard Names on page 194

Configure Sets of Statements

When sets of statements exist in configuration groups, all values are inherited. For example:

```

[edit]
user@host# show
groups {
    basic {
        snmp {
            interface so-1/1/1.0;
        }
    }
}
apply-groups basic;
snmp {
    interface so-0/0/0.0;
}
[edit]
user@host# show | display inheritance
snmp {
    ##
    ## 'so-1/1/1.0' was inherited from group 'basic'
    ##
    interface [ so-0/0/0.0 so-1/1/1.0 ];
}

```

For sets that are not displayed within brackets, all values are also inherited. For example:

```
[edit]
user@host# show
groups {
  worldwide {
    system {
      name-server {
        10.0.0.100;
        10.0.0.200;
      }
    }
  }
}
apply-groups worldwide;
system {
  name-server {
    10.0.0.1;
    10.0.0.2;
  }
}
[edit]
user@host# show | display inheritance
system {
  name-server {
    10.0.0.1;
    10.0.0.2;
    ##
    ## '10.0.0.100' was inherited from group 'worldwide'
    ##
    10.0.0.100;
    ##
    ## '10.0.0.200' was inherited from group 'worldwide'
    ##
    10.0.0.200;
  }
}
```


Configure Interfaces

You can use configuration groups to separate the common interface media parameters from the interface-specific addressing information. The following example places configuration data for ATM interfaces into a group called atm-options:

```
[edit]
user@host# show
groups {
  atm-options {
    interfaces {
      <at-*> {
        atm-options {
          vpi 0 maximum-vcs 1024;
        }
        unit <*> {
          encapsulation atm-snap;
          point-to-point;
          family iso;
        }
      }
    }
  }
}
apply-groups atm-options;
interfaces {
  at-0/0/0 {
    unit 100 {
      vci 0.100;
      family inet {
        address 10.0.0.100/30;
      }
    }
    unit 200 {
      vci 0.200;
      family inet {
        address 10.0.0.200/30;
      }
    }
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  at-0/0/0 {
    ##
    ## "atm-options" was inherited from group "atm-options"
    ##
    atm-options {
      ##
      ## "1024" was inherited from group "atm-options"
      ##
      vpi 0 maximum-vcs 1024;
    }
  }
}
```

```

unit 100 {
  ##
  ## "atm-snap" was inherited from group "atm-options"
  ##
  encapsulation atm-snap;
  ##
  ## "point-to-point" was inherited from group "atm-options"
  ##
  point-to-point;
  vci 0.100;
  family inet {
    address 10.0.0.100/30;
  }
  ##
  ## "iso" was inherited from group "atm-options"
  ##
  family iso;
}
unit 200 {
  ##
  ## "atm-snap" was inherited from group "atm-options"
  ##
  encapsulation atm-snap;
  ##
  ## "point-to-point" was inherited from group "atm-options"
  ##
  point-to-point;
  vci 0.200;
  family inet {
    address 10.0.0.200/30;
  }
  ##
  ## "iso" was inherited from group "atm-options"
  ##
  family iso;
}
}
[edit]
user@host# show | display inheritance | except ##
interfaces {
  at-0/0/0 {
    atm-options {
      vpi 0 maximum-vcs 1024;
    }
    unit 100 {
      encapsulation atm-snap;
      point-to-point;
      vci 0.100;
      family inet {
        address 10.0.0.100/30;
      }
    }
    family iso;
  }
}

```

```

    unit 200 {
        encapsulation atm-snap;
        point-to-point;
        vci 0.200;
        family inet {
            address 10.0.0.200/30;
        }
        family iso;
    }
}

```

Configure Peer Entities

In this example, we create a group `some-isp` that contains configuration data relating to another ISP. We can then insert `apply-group` statements at any point to allow any location in the configuration hierarchy to inherit this data.

```

[edit]
user@host# show
groups {
    some-isp {
        interfaces {
            <ge-*> {
                gigether-options {
                    flow-control;
                }
            }
        }
        protocols {
            bgp {
                group <*> {
                    neighbor <*> {
                        remove-private;
                    }
                }
            }
            pim {
                interface <*> {
                    version 1;
                }
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        apply-groups some-isp;
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
        }
    }
}

```

```

protocols {
  bgp {
    group main {
      neighbor 10.254.0.1 {
        apply-groups some-isp;
      }
    }
  }
  pim {
    interface ge-0/0/0.0 {
      apply-groups some-isp;
    }
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  ge-0/0/0 {
    ##
    ## "gigether-options" was inherited from group "some-isp"
    ##
    gigether-options {
      ##
      ## "flow-control" was inherited from group "some-isp"
      ##
      flow-control;
    }
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
protocols {
  bgp {
    group main {
      neighbor 10.254.0.1 {
        ##
        ## "remove-private" was inherited from group "some-isp"
        ##
        remove-private;
      }
    }
  }
  pim {
    interface ge-0/0/0.0 {
      ##
      ## "1" was inherited from group "some-isp"
      ##
      version 1;
    }
  }
}

```

Establish Regional Configurations

In this example, one group is populated with configuration data that is standard throughout the company, while another group contains regional deviations from this standard.

```
[edit]
user@host# show
groups {
  standard {
    interfaces {
      <t3-*> {
        t3-options {
          compatibility-mode larscom subrate 10;
          idle-cycle-flag ones;
        }
      }
    }
  }
  northwest {
    interfaces {
      <t3-*> {
        t3-options {
          long-buildout;
          compatibility-mode kentrox;
        }
      }
    }
  }
}
apply-groups standard;
interfaces {
  t3-0/0/0 {
    apply-groups northwest;
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  t3-0/0/0 {
    ##
    ## "t3-options" was inherited from group "northwest"
    ##
    t3-options {
      ##
      ## "long-buildout" was inherited from group "northwest"
      ##
      long-buildout;
      ##
      ## "kentrox" was inherited from group "northwest"
      ##
      compatibility-mode kentrox;
      ##
      ## "ones" was inherited from group "standard"
      ##
      idle-cycle-flag ones;
    }
  }
}
```

Select Wildcard Names

You can combine wildcarding and thoughtful use of names in statements to tailor statement values.

```
[edit]
user@host# show
groups {
  mpls-conf {
    protocols {
      mpls {
        label-switched-path <*-major> {
          retry-timer 5;
          bandwidth 155m;
          optimize-timer 60;
        }
        label-switched-path <*-minor> {
          retry-timer 15;
          bandwidth 64k;
          optimize-timer 120;
        }
      }
    }
  }
}
apply-groups mpls-conf;
protocols {
  mpls {
    label-switched-path metro-major {
      to 10.0.0.10;
    }
    label-switched-path remote-minor {
      to 10.0.0.20;
    }
  }
}
[edit]
user@host# show | display inheritance
protocols {
  mpls {
    label-switched-path metro-major {
      to 10.0.0.10;
      ##
      ## "5" was inherited from group "mpls-conf"
      ##
      retry-timer 5;
      #
      ## "155m" was inherited from group "mpls-conf"
      ##
      bandwidth 155m;
      ##
      ## "60" was inherited from group "mpls-conf"
      ##
      optimize-timer 60;
    }
  }
}
```

```

label-switched-path remote-minor {
  to 10.0.0.20;
  ##
  ## "15" was inherited from group "mpls-conf"
  ##
  retry-timer 15;
  ##
  ## "64k" was inherited from group "mpls-conf"
  ##
  bandwidth 64k;
  ##
  ## "120" was inherited from group "mpls-conf"
  ##
  optimize-timer 120;
}
}
}

```

Summary of Configuration Group Statements

The following sections explain each of the configuration group statements. The statements are organized alphabetically.

apply-groups

Syntax `apply-groups [group-name];`

Hierarchy Level All hierarchy levels

Description Apply a configuration group to a specific hierarchy level in a configuration, to have a configuration inherit the statements in the configuration group.

You can specify more than one group name. You must list them in order of inheritance priority. The configuration data in the first group takes priority over the data in subsequent groups.

For routers that support multiple Routing Engines, you can specify `re0` and `re1` as group names. The configuration specified in group `re0` is applied only if the current Routing Engine is in slot 0; likewise, the configuration specified in group `re1` is applied only if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each `re0` or `re1` group contains at a minimum the configuration for the hostname and the management interface (`fxp0`). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

You can include the `apply-groups` statement at any level of the configuration hierarchy.

You can include only one `apply-groups` statement at each specific level of the configuration hierarchy. The `apply-groups` statement at a specific hierarchy level lists the configuration groups to be added to the containing statement's list of configuration groups.

Options	<i>group-name</i> —Names specified on the group statement.
Usage Guidelines	See “Apply a Configuration Group” on page 181.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.
See Also	groups on page 196

groups

Syntax	<pre>groups { group-name { configuration-data; } }</pre>
Hierarchy Level	[edit]
Description	Create a configuration group.
Options	<p><i>configuration-data</i>—The configuration statements that are to be applied elsewhere in the configuration with the <i>apply-groups</i> statement, to have the target configuration inherit the statements in the group.</p> <p><i>group-name</i>—Name of the configuration group. To configure multiple groups, specify more than one <i>group-name</i>. On routers that support multiple Routing Engines, you can also specify two special group names:</p> <ul style="list-style-type: none"> ■ <i>re0</i>—Configuration statements that are to be applied to the Routing Engine in slot 0. ■ <i>re1</i>—Configuration statements that are to be applied to the Routing Engine in slot 1. <p>The configuration specified in group <i>re0</i> is applied only if the current Routing Engine is in slot 0; likewise, the configuration specified in group <i>re1</i> is applied only if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each <i>re0</i> or <i>re1</i> group contains at a minimum the configuration for the hostname and the management interface (<i>fxp0</i>). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.</p>
Usage Guidelines	See “Create a Configuration Group” on page 181.
Required Privilege Level	configure—To enter configuration mode.
See Also	<i>apply-groups</i> on page 195

Chapter 14

Summary of CLI Environment Commands

The following sections explain each of the CLI environment commands. The commands are organized alphabetically.

set cli complete-on-space

Syntax	set cli complete-on-space (off on);
Description	Configure the keys to use for command completion.
Default	When you type a space or tab, the CLI performs command completion.
Options	off—Allow only a tab to be used for command completion. on—Allow either a space or a tab to be used for command completion.
Sample Output	<pre>user@host> set cli com<Space> user@host> set cli complete-on-space off user@host> set cli com<Tab> user@host> set cli complete-on-space on user@host></pre>
Usage Guidelines	See “Set Command Completion” on page 125.
Required Privilege Level	view

set cli idle-timeout

Syntax set cli idle-timeout <minutes>

Description Set the maximum time that an individual session can be idle before the user is logged off the router. The session times out after remaining at the CLI operational mode prompt for the specified time. The session can time out while monitoring log files.

Default If you do not issue this command, and the user's login class does not specify this value, the user is never forced off the system after extended idle times.

Options *minutes*—Maximum idle time.
Range: 0 through 100,000 minutes. Setting it to 0 disables the timeout.

Usage Guidelines See "Set the Idle Timeout" on page 124.

Required Privilege Level view

See Also idle-timeout on page 297

set cli prompt

Syntax set cli prompt *string*

Description Set the prompt to display within the CLI.

Default user@host>

Options *string*—CLI prompt. To include spaces in the prompt, enclose the string in quotation marks.

Sample Output user@host> set cli prompt "cli% "
 cli%

Usage Guidelines See "Set the CLI Prompt" on page 124.

Required Privilege Level view

set cli restart-on-upgrade

Syntax set cli restart-on-upgrade (off | on)

Description For an individual session, set the CLI to prompt you to restart the router after upgrading the software.

Default The CLI prompts you to restart, unless the screen length has been set to 0.

Options off—Disables the prompt.

on—Enables the prompt.

Usage Guidelines See "Set CLI to Prompt after a Software Upgrade" on page 125.

Required Privilege Level view

set cli screen-length

Syntax	set cli screen-length <i>lines</i>
Description	Set the number of lines of text that the screen can display.
Options	<i>lines</i> —Number of lines on the screen. Range: 0 through 100,000 Default: 24 lines
Sample Output	<pre>user@host> set cli screen-length 66 Screen length is set to 66 user@host></pre>
Usage Guidelines	See “Set the Screen Length” on page 124.
Required Privilege Level	view

set cli screen-width

Syntax	set cli screen-width <i>width</i>
Description	Set the number of characters that the screen can display on a single line.
Options	<i>width</i> —Number of columns on the screen. Range: 0 through 100,000 Default: 80 columns
Sample Output	<pre>user@host> set cli screen-width 40 Screen width set to 40 user@host></pre>
Usage Guidelines	See “Set the CLI Prompt” on page 124.
Required Privilege Level	view

set cli terminal

Syntax	set cli terminal <i>terminal-type</i>
Description	Set the terminal type.
Options	<i>terminal-type</i> —Type of terminal that is connected to the port. Values: ansi, vt100, small-xterm, xterm Default: The terminal type is unknown.
Usage Guidelines	See “Set the Terminal Type” on page 124.
Required Privilege Level	view

set date

Syntax set date YYYYMMDDhhmm.ss

Description Set the current date and time on the router.

Options YYYYMMDDhhmm.ss—Date and time to set. YYYY is the four-digit year, MM is the two-digit month, DD is the two-digit date, hh is the two-digit hour, mm is the two-digit minute, and ss is the two-digit second. At a minimum, you must specify the two-digit minute. All other parts of the date and time are optional.

Usage Guidelines See “Set the Current Date and Time” on page 119.

Required Privilege Level view

See Also ntp on page 303, time-zone on page 315

set date ntp

Syntax set date ntp <ntp-server>

Description Use an NTP server to synchronize the current date and time setting on the router.
You do not need to reboot the router when you use the set date ntp command.

Options none—Uses system NTP server list.

ntp-server—IP address of one or more NTP servers to query. When querying more than one server, the IP addresses are enclosed in quotes using the format “ip-address ip-address”, for example, “200.49.40.1 129.127.28.4”.

Usage Guidelines See “Set Date and Time from NTP Servers” on page 119.

Required Privilege Level view

Sample Output: set date ntp (to query one server)

```
user@host> set date ntp 172.17.12.9
14 Sep 22:00:50 ntpdate[20603]: step time server 172.17.12.9 offset 0.000461 sec
```

Sample Output: set date ntp (to query two servers)

```
user@host> set date ntp "200.49.40.1 129.127.28.4"
10 Feb 13:50:21 ntpdate[794]: step time server 129.127.28.4 offset 0.000163 sec
```

show cli

Syntax show cli

Description Display information about how the CLI environment is configured.

Sample Output

```
user@host> show cli
CLI screen length set to 60
CLI screen width set to 80
CLI complete-on-space set to on
user@host>
```

Usage Guidelines See “Display CLI Settings” on page 125.

Required Privilege Level view

show cli history

Syntax show cli history < count>

Description List recent commands that you issued in the CLI and the time they were issued.

If you issue the run show cli history command from configuration mode, the command lists the most recent configuration mode commands that you issued and the time they were issued.

Options count—(Optional) Number of recent commands to display.
Range: 0 through 65,535
Default: 100

Sample Output

```
user@host> show cli history
12:33:39 -- configure
12:42:52 -- show cli history
12:43:02 -- show interfaces terse
12:43:14 -- show interfaces lo0
12:43:20 -- show bgp
12:43:28 -- show bgp next-hop-database
12:43:32 -- show cli history
user@host> configure
...
[edit]
user@host# run show cli history
12:40:08 -- show
12:40:17 -- edit protocols
12:40:27 -- set isis
12:40:29 -- edit isis
12:40:40 -- run show cli history
[edit protocols isis]
user@host#
```

Usage Guidelines See the sections “Display CLI Command History” on page 120 and “Display Configuration Mode Command History” on page 156.

Required Privilege Level view

Chapter 15

Summary of CLI Configuration Mode Commands

The following sections explain each of the CLI configuration mode commands. The commands are organized alphabetically.

activate

Syntax	activate (<i>statement</i> <i>identifier</i>)
Description	Remove the inactive: tag from a statement, effectively adding the statement or identifier back to the configuration. Statements or identifiers that have been activated take effect when you next issue the commit command.
Options	<i>identifier</i> —Identifier from which you are removing the inactive tag. It must be an identifier at the current hierarchy level. <i>statement</i> —Statement from which you are removing the inactive tag. It must be a statement at the current hierarchy level.
Usage Guidelines	See “Deactivate and Reactivate Statements and Identifiers in a Configuration” on page 166.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.
See Also	deactivate on page 206

annotate

Syntax `annotate statement "comment-string"`

Description Add comments to a configuration. You can add comments only at the current hierarchy level.

Any comments you add appear only when you view the configuration by entering the `show` command in configuration mode or the `show configuration` command in operational mode.

Options *comment-string*—Text of the comment. You must enclose it in quotation marks. In the comment string, you can include the comment delimiters `/* */` or `#`. If you do not specify any, the comment string is enclosed with the `/* */` comment delimiters. If a comment for the specified *statement* already exists, it is deleted and replaced with the new comment.

statement—Statement to which you are attaching the comment.

Usage Guidelines See “Add Comments in a Configuration” on page 167.

Required Privilege Level `configure`—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also See the description statement in the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

commit

Syntax commit < and-quit> < check> < confirmed < *minutes*> > < synchronize>

Description Commit the set of changes to the database and cause the changes to take operational effect.

Options and-quit—(Optional) Commit the configuration and, if the configuration contains no errors and the commit succeeds, exit from configuration mode.

check—(Optional) Verify the syntax of the configuration, but do not activate it.

confirmed <*minutes*>—(Optional) Require that the commit be confirmed within the specified amount of time. To confirm a commit, enter either a commit or commit check command. If the commit is not confirmed within the time limit, the configuration rolls back automatically to the precommit configuration.

Range: 1 through 65,535 minutes

Default: 10 minutes

synchronize—(Optional) If your router has two Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the other by issuing the commit synchronize command. The Routing Engine on which you execute this command (request Routing Engine) copies and loads its candidate configuration to the other (responding Routing Engine). Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

**Note**

When you issue the commit synchronize command, you must use the apply-groups re0 and re1 commands. For information about how to use apply groups, see “Apply a Configuration Group” on page 181.

The responding Routing Engine must use JUNOS release 5.0 or higher.

Usage Guidelines See the sections “Verify a Configuration” on page 157, “Commit a Configuration” on page 157, and “Synchronize Routing Engines” on page 160.

Required Privilege Level configure—To enter configuration mode.

copy

Syntax *copy existing-statement to new-statement*

Description Make a copy of an existing statement in the configuration.

Options *existing-statement*—Statement to copy.
new-statement—Copy of the statement.

Usage Guidelines See “Copy a Statement in the Configuration” on page 152.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

deactivate

Syntax *deactivate (statement | identifier)*

Description Add the inactive: tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the commit command.

Options *identifier*—Identifier to which you are adding the inactive: tag. It must be an identifier at the current hierarchy level.
statement—Statement to which you are adding the inactive: tag. It must be a statement at the current hierarchy level.

Usage Guidelines See “Deactivate and Reactivate Statements and Identifiers in a Configuration” on page 166.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also activate on page 203, delete on page 207

delete

Syntax delete < *statement-path*> < *identifier*>

Description Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.

Deleting a statement or an identifier effectively “unconfigures” or disables the functionality associated with that statement or identifier.

If you do not specify *statement-path* or *identifier*, the entire hierarchy starting at the current hierarchy level is removed.

Options *statement-path*—(Optional) Path to an existing statement or identifier. Include this if the statement or identifier to be deleted is not at the current hierarchy level.

identifier—(Optional) Name of the statement or identifier to delete.

Usage Guidelines See “Remove a Statement from the Configuration” on page 150.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also deactivate on page 206

edit

Syntax edit *statement-path*

Description Move inside the specified statement hierarchy. If the statement does not exist, it is created.

You cannot use the edit command to change the value of identifiers. You must use the set command.

Options *statement-path*—Path to the statement.

Usage Guidelines See “Create and Modify the Configuration” on page 142.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also set on page 213

exit

Syntax exit < configuration-mode>

Description Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.

Options none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.

configuration-mode—(Optional) Exit from configuration mode.

Usage Guidelines See “Move among Levels of the Hierarchy” on page 145.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also top on page 214, up on page 214

help

Syntax help (apropos | topic | reference) < *string* >

Description Display help about available configuration statements.

Options apropos—Display all hierarchy levels containing the statement.

reference—Display summary information for the statement.

string—String or regular expression matching configuration statements for which you need help.

topic—(Optional) Display usage guidelines for the statement.

Usage Guidelines See “Get Help Based on a String in a Statement Name” on page 141.

Required Privilege Level configure—To enter configuration mode.

insert

Syntax	insert < <i>statement-path</i> > <i>identifier1</i> (before after) <i>identifier2</i>
Description	Insert an identifier into an existing hierarchy.
Options	<p>after—Place <i>identifier1</i> after <i>identifier2</i>.</p> <p>before—Place <i>identifier1</i> before <i>identifier2</i>.</p> <p><i>identifier1</i>—Existing identifier.</p> <p><i>identifier2</i>—New identifier to insert.</p> <p><i>statement-path</i>—(Optional) Path to the existing identifier.</p>
Usage Guidelines	See “Insert a New Identifier” on page 153.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

load

Syntax	load (replace merge override) (<i>filename</i> terminal)
Description	Load a configuration from an ASCII configuration file or from terminal input. Your current location in the configuration hierarchy is ignored when the load operation occurs.
Options	<p><i>filename</i>—Name of the file to load. For information about specifying the filename, see “How to Specify Filenames and URLs” on page 224.</p> <p>merge—Combine the configuration that is currently shown in the CLI and the configuration in <i>filename</i>.</p> <p>override—Discard the entire configuration that is currently shown in the CLI and load the entire configuration in <i>filename</i>.</p> <p>replace—Look for a replace: tag in <i>filename</i>, delete the existing statement of the same name, and replace it with the configuration in <i>filename</i>.</p> <p>terminal—Use the text you type at the terminal as input to the configuration. Type Ctrl-D to end terminal input.</p>
Usage Guidelines	See “Load a Configuration” on page 162.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

quit

Syntax quit < configuration-mode>

Description Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.

Options none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.

configuration-mode—(Optional) Exit from configuration mode.

Usage Guidelines See “Move among Levels of the Hierarchy” on page 145.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

See Also top on page 214, up on page 214

rename

Syntax rename < *statement-path*> *identifier1* to *identifier2*

Description Rename an existing configuration statement or identifier.

Options *identifier1*—Existing identifier to rename.

identifier2—New name of identifier.

statement-path—(Optional) Path to an existing statement or identifier.

Usage Guidelines See “Rename an Identifier” on page 153.

Required Privilege Level configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

rollback

Syntax rollback < *number*>

Description Return to a previously committed configuration. The software saves the last ten committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command.

The currently operational JUNOS software configuration is stored in the file `juniper.conf`, and the last three committed configurations are stored in the files `juniper.conf.1`, `juniper.conf.2`, and `juniper.conf.3`. These four files are located in the directory `/config`, which is on the router's flash drive. The remaining six previous committed configurations, the files `juniper.conf.4` through `juniper.conf.9`, are stored in the directory `/var/db/config`, which is on the router's hard disk.

Options none—Return to the most recently saved configuration.

number—Configuration to return to.

Range: 0 through 9. The most recently saved configuration is number 0, and the oldest saved configuration is number 9.

Default: 0

Usage Guidelines See “Return to a Previously Committed Configuration” on page 164.

Required Privilege Level rollback—To roll back to configurations other than the one most recently committed.

run

Syntax run *command*

Description Run a top-level CLI command without exiting from configuration mode.

Options *command*—CLI top-level command.

Usage Guidelines See “Run an Operational Mode CLI Command from Configuration Mode” on page 156.

Required Privilege Level configure—To enter configuration mode.

save

Syntax `save filename`

Description Save the configuration to an ASCII file. The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy.

When saving a file to a remote system, the software uses the scp/ssh protocol.

Options *filename*—Name of the saved file. You can specify a filename in one of the following ways:

- *filename*—File in the user's home directory (the current directory) on the local flash disk.
- *path/filename*—File on the local flash disk.
- */var/filename* or */var/path/filename*—File on the local hard disk.
- *a:filename* or *a:path/filename*—File on the local drive. The default path is */* (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.
- *hostname:/path/filename*, *hostname:filename*, *hostname:path/filename*, or *scp://hostname/path/filename*—File on an scp/ssh client. This form is not available in the worldwide version of the JUNOS software. The default path is the user's home directory on the remote system. You can also specify *hostname* as *username@hostname*.
- *ftp://hostname/path/filename*—File on an FTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. The default path is the user's home directory. To specify an absolute path, the path must start with *%2F*; for example, *ftp://hostname/%2Fpath/filename*. To have the system prompt you for the password, specify *prompt* in place of the password. If a password is required, and you do not specify the password or prompt, an error message is displayed:


```
user@host > file copy ftp://username@ftp.hostname.net//filename
file copy ftp.hostname.net: Not logged in.
user@host > file copy ftp://username:prompt@ftp.hostname.net//filename
Password for username@ftp.hostname.net:
```
- *http://hostname/path/filename*—File on an HTTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. If a password is required and you omit it, you are prompted for it.
- *re0:/path/filename* or *re1:/path/filename*—File on a local Routing Engine.

Usage Guidelines See "Save a Configuration to a File" on page 161.

Required Privilege Level *configure*—To enter configuration mode.

set

Syntax	<code>set < statement-path> identifier</code>
Description	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change.
Options	<p><i>identifier</i>—Name of the statement or identifier to set.</p> <p><i>statement-path</i>—(Optional) Path to an existing statement hierarchy level. If that hierarchy level does not exist, it is created.</p>
Usage Guidelines	See “Create and Modify the Configuration” on page 142.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.
See Also	edit on page 207

show

Syntax	<code>show < statement-path> < identifier></code>
Description	Display the current configuration.
Options	<p><i>none</i>—Display the entire configuration at the current hierarchy level.</p> <p><i>identifier</i>—(Optional) Display the configuration for the specified identifier.</p> <p><i>statement-path</i>—(Optional) Display the configuration for the specified statement hierarchy path.</p>
Usage Guidelines	See “Display the Current Configuration” on page 148.
Required Privilege Level	configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

status

Syntax	<code>status</code>
Description	Display the users currently editing the configuration.
Usage Guidelines	See “Display Users Currently Editing the Configuration” on page 150.
Required Privilege Level	configure—To enter configuration mode.

top

Syntax top < *configuration-command*>

Description Return to the top level of configuration command mode, which is indicated by the [edit] banner.

Option *configuration-command*—Issue configuration mode commands from the top of the hierarchy.

Usage Guidelines See “Move among Levels of the Hierarchy” on page 145 and “Issue Relative Configuration Commands” on page 147.

Required Privilege Level configure—To enter configuration mode.

See Also exit on page 208, up on page 214

up

Syntax up < *number*> < *configuration-command*>

Description Move up one level in the statement hierarchy.

Options none—Move up one level in the configuration hierarchy.

number—(Optional) Move up the specified number of levels in the configuration hierarchy.

configuration-command—Issue configuration mode commands from a location higher in the hierarchy.

Usage Guidelines See “Move among Levels of the Hierarchy” on page 145 and “Issue Relative Configuration Commands” on page 147.

Required Privilege Level configure—To enter configuration mode.

See Also exit on page 208, top on page 214

Chapter 16

Summary of CLI Operational Mode Commands

The following sections explain each of the CLI operational mode commands. The commands are organized alphabetically.

clear

Syntax	clear (arp bgp chassis firewall igmp interfaces isis ldp log mpls msdp multicast ospf pim rip route rsvp snmp system vrrp)
Description	Clear statistics and protocol database information.
Usage Guidelines	The various clear commands are discussed in the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	clear

configure

Syntax	configure configure exclusive configure private
Description	Enter configuration mode.
Usage Guidelines	See “Enter Configuration Mode” on page 131.
Required Privilege Level	configure

file

Syntax	file (copy delete list rename show)
Description	Copy files to and from the router.
Usage Guidelines	See the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	maintenance

monitor

Syntax monitor (start | stop | interface | list | traffic)

Description Monitor a log file or interface traffic in real time.

Usage Guidelines See the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level Depends on the specific command.

ping

Syntax ping

Description Check the reachability of network hosts.

Usage Guidelines See the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level network

update

Syntax update

Description Updates private candidate configuration with a copy of the most recently committed configuration, including your private changes.

Usage Guidelines See the “Update the Configure Private Configuration” on page 135.



Note

The update command is only available when you are in configure private mode.

| (pipe)

Syntax	(compare count display <detail inheritance xml> except <i>pattern</i> find <i>pattern</i> hold match <i>pattern</i> no-more resolve <full-names> save <i>filename</i> trim <i>columns</i>)
Description	Filter the output of an operational mode or a configuration mode command.
Options	<p>compare (filename rollback <i>n</i>)—(configuration mode only, and only with the show command.) Compare configuration changes with another configuration file.</p> <p>count—Display the number of lines in the output.</p> <p>display—Display additional information about the configuration contents.</p> <ul style="list-style-type: none"> ■ detail—(Configuration mode only) Display configuration data detail. ■ inheritance—(Configuration mode only) Display inherited configuration data and source group. ■ xml—(Operational mode only) Display XML content of the command. <p>except <i>pattern</i>—Ignore text matching a regular expression when searching the output. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks.</p> <p>find <i>pattern</i>—Display the output starting at the first occurrence of text matching a regular expression. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks (" ").</p> <p>hold—Hold text without exiting the --More-- prompt.</p> <p>match <i>pattern</i>—Search for text matching a regular expression. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks.</p> <p>no-more—Display output all at once rather than one screen at a time.</p> <p>resolve—Convert IP addresses into domain name server (DNS) names. Truncates to fit original size unless full-names specified. To prevent the names from being truncated, use the full-name option.</p> <p>save <i>filename</i>—Save the output to a file or URL. For information about specifying the filename, see “How to Specify Filenames and URLs” on page 224.</p> <p>trim <i>columns</i>—Trim specified number of columns from the start line.</p>
Usage Guidelines	See “Filter Command Output” on page 110.

quit

Syntax	quit
Description	Exit from the CLI to a UNIX shell.
Required Privilege Level	shell and maintenance
See Also	start on page 219

request

Syntax request system (reboot | halt | software | snapshot)

Description Stop or reboot the router, load software packages, and back up the router's file systems.

Usage Guidelines See the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level maintenance

restart

Syntax restart (fpc | interface-control | mib-process | routing | sampling | sfm | snmp | soft)

Description Restart router software processes.

Usage Guidelines See the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level reset

set

Syntax set (chassis | cli | date)

Description Configure chassis and CLI properties and the router's date and time.

Usage Guidelines See "Control the CLI Environment" on page 123 and "Set the Current Date and Time" on page 119. For information about setting chassis properties, see the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level view

show

Syntax show (aps | arp | as-path | bgp | chassis | cli | configuration | connections | dvmrp | firewall | host | igmp | interfaces | isis | ldp | log | mpls | msdpl | multicast | ntp | ospf | pfe | pim | policy | ripl | route | rsvp | sap | snmp | system | task | ted | version | vrrp)

Description Show information about all aspects of the software, including interfaces and routing protocols.

Usage Guidelines The various show commands are discussed in the *JUNOS Internet Software Operational Mode Command Reference*.

Required Privilege Level Depends on the specific command.

ssh

Syntax	ssh
Description	Open a secure shell to another host.
Usage Guidelines	See the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	network

start

Syntax	start shell
Description	Start a UNIX shell on the router.
Usage Guidelines	See the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	shell and maintenance

telnet

Syntax	telnet
Description	Establish a Telnet session to another host.
Usage Guidelines	See the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	network

test

Syntax	test (configuration interface msdp policy)
Description	Run various diagnostic debugging commands.
Usage Guidelines	The various test commands are discussed in the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	Depends on the specific command.

traceroute

Syntax	traceroute
Description	Trace the route to a remote host.
Usage Guidelines	See the <i>JUNOS Internet Software Operational Mode Command Reference</i> .
Required Privilege Level	network

Part 4

System Management

- System Management Overview on page 223
- System Management Configuration Statements on page 229
- Configure Basic System Management on page 233
- Configure System Authentication on page 241
- Configure User Access on page 253
- Configure Time on page 265
- Configure System Logging on page 271
- Configure Miscellaneous System Management Features on page 277
- Summary of System Management Configuration Statements on page 285

Chapter 17

System Management Overview

The JUNOS software provides a variety of parameters that allow you to configure system management functions, including the router's host name, address, and domain name; the addresses of DNS servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; and properties of the router's auxiliary and console ports.

This chapter discusses the following topics, which provide background information related to configuring system management:

- How to Specify IP Addresses, Network Masks, and Prefixes on page 223
- How to Specify Filenames and URLs on page 224
- Directories on the Router on page 225
- Tracing and Logging Operations on page 225
- Protocol Authentication on page 226
- User Authentication on page 227

How to Specify IP Addresses, Network Masks, and Prefixes

Many statements in the JUNOS software configuration include an option to specify an IP address or route prefix. In this manual, this option is represented in one of the following ways:

- *network/prefix-length*—Network portion of the IP address, followed by a slash and the destination prefix length (previously called the subnet mask). For example, 10.0.0.1/8.
- *network*—IP address. An example is 10.0.0.2.
- *destination-prefix/prefix-length*—Route prefix, followed by a slash and the destination prefix length. For example, 192.168.1.10/32.

You enter all IP addresses in classless mode. You can enter the IP address with or without a prefix length, in standard dotted notation (for example, 1.2.3.4), or hexadecimal notation as a 32-bit number in network-byte order (for example, 0x01020304). If you omit any octets, they are assumed to be zero. Specify the prefix length as a decimal number in the range 1 through 32.

How to Specify Filenames and URLs

In some CLI commands and configuration statements—including file copy, load, save, set system login user *user-name* authentication *load-key-file*, and request system software add—you can include a filename. You can specify a filename or URL in one of the following ways:

- *filename*—File in the user's home directory (the current directory) on the local flash disk.
- *path/filename*—File on the local flash disk.
- */var/filename* or */var/path/filename*—File on the local hard disk.
- *a:filename* or *a:path/filename*—File on the local drive. The default path is */* (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.
- *hostname:/path/filename*, *hostname:filename*, *hostname:path/filename*, or *scp://hostname/path/filename*—File on an scp/ssh client. This form is not available in the worldwide version of the JUNOS software. The default path is the user's home directory on the remote system. You can also specify *hostname* as *username@hostname*.
- *ftp://hostname/path/filename*—File on an FTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. The default path is the user's home directory. To specify an absolute path, the path must start with *%2F*; for example, *ftp://hostname/%2Fpath/filename*. To have the system prompt you for the password, specify *prompt* in place of the password. If a password is required, and you do not specify the password or prompt, an error message is displayed:


```

user@host > file copy ftp://username@ftp.hostname.net//filename
file copy ftp.hostname.net: Not logged in.
user@host > file copy ftp://username:prompt@ftp.hostname.net//filename
Password for username@ftp.hostname.net:
      
```
- *http://hostname/path/filename*—File on an HTTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. If a password is required and you omit it, you are prompted for it.
- *re0:/path/filename* or *re1:/path/filename*—File on a local Routing Engine.

Directories on the Router

JUNOS software files are stored in the following directories on the router:

- **/config**—This directory is located on the primary boot device, that is, on the drive from which the router booted (generally the flash disk, device wd0). This directory contains the current operational router configuration and the last three committed configurations, in the files `juniper.conf`, `juniper.conf.1`, `juniper.conf.2`, and `juniper.conf.3`, respectively.
- **/var**—This directory is always located on the hard disk (device wd2). It contains the following subdirectories:
 - **/var/home**—Contains users' home directories, which are created when you create user access accounts. For users using secure shell (SSH) authentication, their `.ssh` file, which contains their SSH key, is placed in their home directory. When a user saves or loads a configuration file, that file is loaded from their home directory unless the user specifies a full path name.
 - **/var/db/config**—Up to six additional previous versions of committed configurations, which are stored in the files `juniper.conf.4` through `juniper.conf.9`.
 - **/var/log**—Contains system log and tracing files.
 - **/var/tmp**—Contains core files. The software saves the current core file (0) and the four previous core files, which are numbered 1 through 4 (from newest to oldest).
- **/altroot**—When you back up the currently running and active file system partitions on the router to standby partitions using the `request system snapshot` command, the root file system (`/`) is backed up to `/altroot`. Normally, the root directory is on the flash disk and `/altroot` is on the hard drive.
- **/altconfig**—When you back up the currently running and active file system partitions on the router to standby partitions using the `request system snapshot` command, the `/config` directory is backed up to `/altconfig`. Normally, the `/config` directory is on the flash disk and `/altconfig` is on the hard drive.

Each router ships with removable media (device wfd0) that contains a backup copy of the JUNOS software.

Tracing and Logging Operations

Tracing and logging operations allow you to track events that occur in the router—both normal router operations and error conditions—and to track the packets that are generated by or passed through the router. The results of tracing and logging operations are placed in files in the `/var/log` directory on the router.

Logging operations use a UNIX syslog mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging into or out of the router. You configure these operations by using the `syslog` statement at the `[edit system]` hierarchy level, as described in "Configure System Logging" on page 271, and by using the `options` statement at the `[edit routing-options]` hierarchy level, as described in the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions. You configure tracing operations using the `traceoptions` statement. You can define tracing operations in different portions of the router configuration:

- **Global tracing operations**—Define tracing for all routing protocols. You define these tracing operations at the `[edit routing-options]` hierarchy level of the configuration. For more information, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.
- **Protocol-specific tracing operations**—Define tracing for a specific routing protocol. You define these tracing operations in the `[edit protocol]` hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global `traceoptions` statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.
- **Tracing operations within individual routing protocol entities**—Some protocols allow you to define more granular tracing operations. For example, in BGP, you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.
- **Interface tracing operations**—Define tracing for individual router interfaces and for the interface process itself. You define these tracing operations at the `[edit interfaces]` hierarchy level of the configuration as described in the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Protocol Authentication

Some IGP (IS-IS, OSPF, and RIP) and RSVP allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- **Simple authentication (IS-IS, OSPF, and RIP)**—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you *not* use this authentication method.
- **MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)**—MD5 creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (" ").

User Authentication

The JUNOS software supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log into the router.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router using Telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router, and the server runs on a remote network system. For TACACS+ , the JUNOS software supports authentication but does not support authorization.

You can configure the router to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the JUNOS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

Chapter 18

System Management Configuration Statements

To configure system management, you can include the following statements in the configuration:

```
system {
  authentication-order [ authentication-methods ];
  backup-router address <destination destination-address>;
  compress-configuration-files;
  default-address-selection;
  dhcp-relay {
    disable;
    maximum-hop-count;
    minimum-wait-time seconds;
    server [ address ];
    interface interface-group {
      no-listen;
      maximum-hop-count;
      minimum-wait-time seconds;
      server [ address ];
    }
  }
}
diag-port-authentication (encrypted-password "password" | plain-text-password);
domain-name domain-name;
domain-search [ domain-list ];
host-name host-name;
location {
  altitude feet;
  country-code code;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  vcoord vertical-coordinate;
}
login {
  message text;
  class class-name {
    allow-commands "regular-expression";
    allow-configuration "regular-expression";
    deny-commands "regular-expression";
    deny-configuration "regular-expression";
    idle-timeout minutes;
    permissions [ permissions ];
  }
}
```

```

user user-name {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
}
mirror-flash-on-disk;
name-server {
    address;
}
no-redirects;
no-saved-core-context;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}
ports {
    auxiliary {
        type terminal-type;
    }
    console {
        type terminal-type;
    }
}
processes {
    inet-process (enable | disable) failover (alternate-media | other-routing-engine);
    interface-control (enable | disable) failover (alternate-media | other-routing-engine);
    mib-process (enable | disable) failover (alternate-media | other-routing-engine);
    ntp (enable | disable) failover (alternate-media | other-routing-engine);
    routing (enable | disable) failover (alternate-media | other-routing-engine);
    snmp (enable | disable) failover (alternate-media | other-routing-engine);
    watchdog (enable | disable) failover (alternate-media | other-routing-engine) timeout seconds;
}
radius-server server-address {
    port number;
    retry number;
    secret password;
    timeout seconds;
}
root-authentication {
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
}
services {
    finger <connection-limit limit> <rate-limit limit>;
    ftp <connection-limit limit> <rate-limit limit>;
    rlogin <connection-limit limit> <rate-limit limit>;
    ssh <connection-limit limit> <rate-limit limit>;
    telnet <connection-limit limit> <rate-limit limit>;
}

```

```

static-host-mapping {
    host-name {
        inet [ address ];
        sysid system-identifier;
        alias [ alias ];
    }
}
syslog {
    file filename {
        facility level;
        archive {
            files number;
            size size;
            (world-readable | no-world-readable);
        }
    }
    host hostname {
        facility level;
        facility-override facility;
        log-prefix string;
    }
    user (username | *) {
        facility level;
    }
    console {
        facility level;
    }
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
}
tacplus-server server-address {
    secret password;
    single-connection;
    timeout seconds;
}
time-zone time-zone;
}

```


Chapter 19

Configure Basic System Management

This chapter discusses the following topics:

- Configure the Router's Name and Addresses on page 233
- Configure the Router's Domain Name on page 235
- Configure Which Domains to Search on page 236
- Configure a DNS Name Server on page 236
- Configure a Backup Router on page 237
- Configure Flash Disk Mirroring on page 238
- Configure the System Location on page 238
- Configure the Root Password on page 239
- Compress the Current Configuration File on page 240

Configure the Router's Name and Addresses

For the router, you can do the following:

- Configure the Router's Name on page 233
- Map the Router's Name to IP Addresses on page 234
- Configure an ISO Sysid on page 234

There is an example showing how to configure a router's name, IP address, and sysid on page 235.

Configure the Router's Name

To configure the router's name, include the `host-name` statement at the [edit system] hierarchy level:

```
[edit system]  
host-name host-name;
```

Map the Router's Name to IP Addresses

To map a router's host name to one or more IP addresses, include the `inet` statement at the [edit system static-host-mapping *host-name*] hierarchy level:

```
[edit system]
static-host-mapping {
  host-name {
    inet [ address ];
    alias [ alias ];
  }
}
```

The *host-name* is the name you specified in the host-name statement.

For each host, you can specify one or more aliases.

Configure an ISO Sysid

For IS-IS to operate on the router, you must configure a system identifier (sysid). The sysid is commonly the Media Access Control (MAC) address or the IP address expressed in binary-coded decimal (BCD). For more information, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

To configure an ISO sysid, include the `sysid` statement at the [edit system static-host-mapping *host-name*] hierarchy level:

```
[edit system]
static-host-mapping {
  host-name {
    sysid system-identifier ;
  }
}
```

The *host-name* is the name you specified in the host-name statement.

system-identifier is the ISO sysid. It is the 6-byte sysid portion of the IS-IS Network Service Access Point (NSAP). We recommend that you use the host's IP address represented in binary-coded decimal (BCD) format. For example, the IP address 192.168.1.77 would be 1921.6800.1077 in BCD.

Example: Configure a Router's Name, IP Address, and Sysid

Configure the router's name, map the name to an IP address and alias, and configure a sysid:

```
[edit]
user@host# set system host-name router-sj1
[edit]
user@host# set system static-host-mapping router-sj1 inet 192.168.1.77
[edit]
user@host# set system static-host-mapping router-sj1 alias sj1
[edit]
user@host# set system static-host-mapping router-sj1 sysid 1921.6800.1077
[edit]
user@host# show
system {
    host-name router-sj1;
    static-host-mapping {
        router-sj1 {
            inet 192.168.1.77;
            alias sj1;
            sysid 1921.6800.1077;
        }
    }
}
```

Configure the Router's Domain Name

For each router, you should configure the name of the domain in which the router is located. This is the default domain name that is appended to host names that are not fully qualified. To configure the domain name, include the domain-name statement at the [edit system] hierarchy level:

```
[edit system]
domain-name domain-name;
```

Example: Configure the Router's Domain Name

Configure the router's domain name:

```
[edit]
user@host# set system domain-name company.net
[edit]
user@host# show
system {
    domain-name company.net;
}
```

Configure Which Domains to Search

If your router is included in several different domains, you can configure those domain names to be searched.

To configure more than one domain to be searched, include the domain-search statement at the [edit system] hierarchy level:

```
[edit system]
domain-search [domain-list];
```

The domain list can contain up to six domain names, with a total of up to 256 characters.

Example: Configure Which Domains to Search

Configure two domains to be searched:

```
[edit system]
domain-search [domainone.net domainonealternate.com]
```

Configure a DNS Name Server

To have the router resolve host names into addresses, you must configure one or more DNS name servers by including the name-server statement at the [edit system] hierarchy level:

```
[edit system]
name-server {
    address;
}
```

Example: Configure a DNS Name Server

Configure two DNS name servers:

```
[edit]
user@host# set system name-server 192.168.1.253
[edit]
user@host# set system name-server 192.168.1.254
[edit]
user@host# show
system {
    name server {
        192.168.1.253;
        192.168.1.254;
    }
}
```


Configure a Backup Router

During the time that the router is booting, the routing protocol process (RPD) is not running; therefore, the router has no static or default routes. To allow the router to boot and to ensure that the router is reachable over the network if the routing protocol process fails to start properly, you configure a backup router, which is a router that is directly connected to the local router (that is, on the same subnet).

To configure a backup router, include the `backup-router` statement at the `[edit system]` hierarchy level:

```
[edit system]
  backup-router address <destination destination-address>;
```

By default, all hosts (default route) are reachable through the backup router. To eliminate the risk of installing a default route in the forwarding table, include the `destination` option, specifying an address that is reachable through the backup router. Specify the address in the format *network/mask-length* so that the entire network is reachable through the backup router.

When the routing protocols start, the address of the backup router is removed from the local routing and forwarding tables. To have the address remain in these tables, configure a static route for that address by including the `static` statement at the `[edit routing-options]` hierarchy level.

Example: Configure a Backup Router

Configure a backup router and have its address remain in the routing and forwarding tables:

```
[edit]
system {
  backup-router 192.168.1.254 destination 208.197.1.0/24;
}
routing-options {
  static {
    route 208.197.1.0/24 {
      gateway 192.168.1.254;
      retain;
    }
  }
}
```

Configure Flash Disk Mirroring

You can direct the hard drive to automatically mirror the contents of the compact flash. When you issue the `mirror-flash-on-disk` statement, the hard drive maintains a synchronized mirror copy of the compact-flash contents. Data written to the compact flash is simultaneously updated in the mirrored copy of the hard drive. If the flash drive fails to read data, the hard drive automatically retrieves its mirrored copy of the flash disk.



Caution

We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the `request system snapshot` command while flash disk mirroring is enabled.

To configure the mirroring of the compact flash to the hard disk, include the `mirror-flash-on-disk` statement at the `[edit system]` hierarchy level:

```
[edit system]
mirror-flash-on-disk;
```



Note

After you have enabled or disabled the `mirror-flash-on-disk` statement, you must reboot the router for your changes to take effect. To reboot, issue the `request system reboot` command.

Configure the System Location

To configure the physical location of the system, include the `location` statement at the `[edit system]` hierarchy level:

```
[edit system]
location {
  altitude feet;
  country-code code;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  vcoord vertical-coordinate;
}
```

Configure the Root Password

The JUNOS software is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log into the router as the user “root” with no password. After you log in, you should configure the root (superuser) password by including the root-authentication statement at the [edit system] hierarchy level:

```
[edit system]
root-authentication {
  (encrypted-password "password"| plain-text-password);
  ssh-rsa "public-key";
  ssh-dsa "public-key";
}
```

If you configure the plain-text-password option, you are prompted to enter and confirm the password:

```
[edit system]
user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

To load an ssh key file, enter the load-key-file command. This command loads RSA (ssh version 1) and DSA (ssh version 2) public keys. You can also configure a user to use ssh-rsa and ssh-dsa keys.

If you load the ssh keys file, the contents of the file are copied into the configuration immediately after you enter the load-key-file statement. To view the ssh keys entries, use the configuration mode show command. For example:

```
[edit system]
user@host# set root-authentication load-key-file my-host:.ssh/identity.pub
.file.19692          |      0 KB |   0.3 KB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
  ssh-rsa "1024 35 972763820408425105546822675724986424163032220740496252839
03820386901415845349641700196106083587229615634757849182736033612764418
74265946893207739108344810126831259577226254616679992783161235004386609
15866283822489746732605661192181489539813965561563786211940327687806538
16960202749164163735913269396344008443 boojum@juniper.net"; # SECRET-DATA
}
```

Example: Configure the Root Password

Configure an encrypted password:

```
[edit]
user@host# set system root-authentication encrypted-password "$1$14c5.$sBopasddsdfs0"
[edit]
user@host# show
system {
  root-authentication {
    encrypted-password "$1$14c5.$sBopasddsdfs0";
  }
}
```

Configure a plain-text password:

```
[edit]
user@host# set system root-authentication plain-text-password
New password: type root password
Retype new password: retype root password
[edit]
user@host# show
system {
  root-authentication {
    encrypted-password "$1$14c5.$sBopasddsdfs0";
  }
}
```

Compress the Current Configuration File

By default, the current operational configuration file is uncompressed, and is stored in the file `juniper.conf`, in the `/config` file system, along with the last three committed versions of the configuration. However, with large networks, the current configuration file might exceed the available space in the `/config` file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. When the current operational configuration file reaches 3 MB in size, you might want to begin compressing the file. To determine the size of the files in the `/config` file system, issue the file `list /config detail` command.

To compress the current configuration file, include the `compress-configuration-files` statement at the `[edit system]` hierarchy level:

```
[edit system]
compress-configuration-files;
```

The current configuration file is compressed on the second commit of the configuration after the first commit is made to include the `compress-configuration-files` statement:

```
[edit system]
user@host# set compress-configuration-files
user@host# commit
commit complete
user@host# commit
commit complete
```

For more information about how configurations are stored, see “How the Configuration Is Stored” on page 130.

Chapter 20

Configure System Authentication

You can configure the router to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the router. If you set up both authentication methods, you also can configure which the router will try first.

When configuring system authentication, you can do the following:

- Configure RADIUS Authentication on page 241
- Configure TACACS+ Authentication on page 243
- Configure Template Accounts for RADIUS and TACACS+ Authentication on page 245
- Configure the Authentication Order on page 248

For examples of configuring system authentication, see “Examples: Configure System Authentication” on page 249.

Configure RADIUS Authentication

To use RADIUS authentication on the router, configure information about one or more RADIUS servers on the network by including the radius-server statement at the [edit system] hierarchy level:

```
[edit system]
radius-server server-address {
  port number;
  secret password;
  retry number;
  timeout seconds;
}
```

In *server-address*, specify the address of the RADIUS server.

You can specify a port number on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2138).

You must specify a password in the secret statement. Passwords can contain spaces. The secret used by the local router must match that used by the server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router attempts to contact a RADIUS authentication server (in the retry statement). By default, the router waits 3 seconds. You can configure this to be a value in the range 1 through 90 seconds. By default, the router retries connecting to the server 3 times. You can configure this to be a value in the range 1 through 10 times.

To configure multiple RADIUS servers, include multiple radius-server statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in “Configure Template Accounts for RADIUS and TACACS+ Authentication” on page 245.

Configure Juniper Networks-Specific RADIUS Attributes

The JUNOS software supports the configuration of Juniper Networks-specific RADIUS attributes. These attributes are known as vendor-specific attributes and are described in RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*. These Juniper Networks-specific attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 8 lists the Juniper Networks-specific attributes you can configure.

Table 8: Juniper Networks-Specific RADIUS Attributes

Name	Description	Type	Length	String
Juniper-Local-User-Name	Indicates the name of the user template used by this user when logging into a device. This attribute is used only in Access-Accept packets.	1	≥3	One or more octets containing printable ASCII characters.
Juniper-Allow-Commands	Contains an extended regular expression that allows the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	2	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
Juniper-Allow-Configuration	Contains an extended regular expression that allows the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	4	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	5	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.

Configure TACACS+ Authentication

To use TACACS+ authentication on the router, configure information about one or more TACACS+ servers on the network by including the `tacplus-server` statement at the [edit system] hierarchy level:

```
[edit system]
tacplus-server server-address {
  secret password;
  single-connection;
  timeout seconds;
}
```

In `server-address`, specify the address of the TACACS+ server.

You must specify a secret (password) that the local router passes to the TACACS+ client by means of the `secret` statement. Secrets can contain spaces. The secret used by the local router must match that used by the server.

As another option, you can specify the length of time that the local router waits to receive a response from a TACACS+ server (in the `timeout` statement). By default, the router waits 3 seconds. You can configure this to be a value in the range 1 through 90 seconds.

Optionally, you can have the software maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, thus optimizing attempts to connect to a TACACS+ server. To do this, include the `single-connection` statement.



Note

Early versions of the TACACS+ server do not support the `single-connection` option. If you specify this option and the server does not support it, the JUNOS software will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple `tacplus-server` statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the `user` statement at the [edit system login] hierarchy level, as described in “Configure Template Accounts for RADIUS and TACACS+ Authentication” on page 245.

Configure Juniper Networks-Specific TACACS+ Attributes

The TACACS attributes listed in Table 9 are specific to Juniper Networks. They are specified in the TACACS+ server configuration file on a per-user basis. The JUNOS software retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run JUNOS with TACACS+.

To specify these attributes, include a service statement in the TACACS+ server configuration file of the following form:

```
service = junos-exec {
    local-user-name = <username-local-to-router>
    allow-commands = "<allow-commands-regexp>"
    allow-configuration = "<allow-configuration-regexp>"

    deny-commands = "<deny-commands-regexp>"
    deny-configuration = "<deny-configuration-regexp>"
}
```

This service statement can appear in a user or group statement.

Table 9: Juniper Networks-Specific TACACS+ Attributes

Name	Description	Length	String
local-user-name	Indicates the name of the user template used by this user when logging into a device.	≥3	One or more octets containing printable ASCII characters.
allow-commands	Contains an extended regular expression that allows the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
deny-commands	Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
allow-configuration	Contains an extended regular expression that allows the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
deny-configuration	Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.

Configure Template Accounts for RADIUS and TACACS+ Authentication

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the CLI username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

This section discusses the following topics:

- Remote Template Accounts on page 245
- Local User Template Accounts on page 246

Remote Template Accounts

By default, the JUNOS software uses the remote template accounts when:

- The authenticated user does not exist locally on the router
- The authenticated user's record in the authentication server specifies local user, or the specified local user does not exist locally on the router

To configure the remote template account, include the username remote and specify the privileges you want to provide to these remote users at the [edit system login user] hierarchy level:

```
[edit]
system {
  login {
    user remote {
      full-name "All remote users";
      uid uid-value;
      class class-name;
    }
  }
}
```

To configure different access privileges for users who share the remote template account, include the allow-commands and deny-commands commands in the authentication server configuration file. For information about how to define access privileges on the authentication server, see “Configure Juniper Networks-Specific RADIUS Attributes” on page 242 and “Configure Juniper Networks-Specific TACACS+ Attributes” on page 244.

For information about creating user accounts, see “Configure User Accounts” on page 262. For an example of how to configure a template account, see “Examples: Configure System Authentication” on page 249.

Local User Template Accounts

You use local user template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the router and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, the JUNOS software issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the JUNOS software, which then determines whether a local username is specified for that login name (local-username for TACACS+ , Juniper-Local-User for RADIUS). If so, the JUNOS software selects the appropriate local user template locally configured on the router. If a local user template does not exist for the authenticated user, the router defaults to the remote template.

To configure different access privileges for users who share the local user template account, include the `allow-commands` and `deny-commands` commands in the authentication server configuration file. For information about how to configure access privileges on the authentication server, see "Configure Juniper Networks-Specific RADIUS Attributes" on page 242 and "Configure Juniper Networks-Specific TACACS+ Attributes" on page 244.

For information about creating user accounts, see "Configure User Accounts" on page 262. For an example of how to configure a template account, see "Examples: Configure System Authentication" on page 249.

To configure the local user template, include the local username and specify the privileges you want to provide to these local users at the `[edit system login user]` hierarchy level:

```
[edit]
system {
  login {
    user local-user-name {
      full-name "local user account";
      uid uid-value;
      class class-name;
    }
  }
}
```

Local User Template Example:

In this example, you configure the sales and engineering local user templates:

```
[edit]
system {
  login {
    user sales {
      uid uid-value;
      class class-name;
    }
    user engineering {
      uid uid-value;
      class class-name;
    }
  }
}
```

Now you configure users on the TACACS+ authentication server:

```

user = simon {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "configure"
    deny-commands = "shutdown"
  }
}
user = rob {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "(request system) | (show rip neighbor)"
    deny-commands = "<^clear"
  }
}
user = harold {
  ...
  service = junos-exec {
    local-user-name = engineering
    allow-commands = "monitor | help | show | ping | traceroute"
    deny-commands = "configure"
  }
}
user = jim {
  ...
  service = junos-exec {
    local-user-name = engineering
    allow-commands = "show bgp neighbor"
    deny-commands = "telnet | ssh"
  }
}

```

When the login users simon and rob are authenticated, they use the sales local user template. When login users harold and jim are authenticated, they use the engineering local user template.



Note

Permission bits override allow and deny commands.

Configure the Authentication Order

If you configure the router to be both a RADIUS and TACACS+ client (by including the `radius-server` and `tacplus-server` statements), you can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying that a user can access the router. For each login attempt, the JUNOS software tries the authentication methods in order, starting with the first one, until the password matches.

To configure the authentication order, include the `authentication-order` statement at the `[edit system]` hierarchy level:

```
[edit system]
authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

- `radius`—Verify the user using RADIUS authentication services.
- `tacplus`—Verify the user using TACACS+ authentication services.
- `password`—Verify the user using the password configured for the user with the authentication statement at the `[edit system login user]` hierarchy level.

If you do not include the `authentication-order` statement, users are verified based on their configured passwords.

Example: Remove an Ordered Set from the Authentication Order

Delete the `radius` statement from the authentication order:

```
[edit system]
delete system authentication-order radius
```

For more information about how to remove a statement from the configuration, see “Remove a Statement from the Configuration” on page 150.

Example: Insert an Order Set in the Authentication Order

Insert the `tacplus` statement after the `radius` statement:

```
[edit system]
insert system authentication-order tacplus after radius
```

For more information about how to modify a portion of the configuration in which the statement order matters, see “Insert a New Identifier” on page 153.

Examples: Configure System Authentication

The following example allows logins only by the individual user Philip, and by users who have been authenticated by a remote RADIUS server. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router. However, if the RADIUS server is not available, the user's login name has a local password, and the user enters that password, the user is authenticated (using the password authentication method) and allowed access to the router. For more information about the password authentication method, see "Example 3: Default to Local User Password Authentication, RADIUS" on page 251.

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the superuser class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the same privileges for the operator class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class superuser;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```



For authorization purposes, you can use a template account to create single accounts that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see "Configure Template Accounts for RADIUS and TACACS+ Authentication" on page 245.

Configuring a single remote user template account requires that all users without individual configuration entries share the same class and UID. When you are using RADIUS and Telnet or RADIUS and ssh together, you can specify a different template user other than the remote user.

To configure an alternate template user, specify the “User-Name” parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample JUNOS configuration:

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class superuser;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class operator;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and user name “operator”
- User Darius with password “redhead” and user name “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

Local User Fallback Mechanism

The JUNOS software provides a local user fallback mechanism (password authentication method) that enables users to log in to the router when no TACACS+ or RADIUS authentication servers is available. The following examples illustrate how this mechanism works:

Example 1: Insert Password into the Authentication Order

If you specify the following authentication order:

```
[edit]
system authentication-order [tacplus password];
```

the JUNOS software first uses the authentication method TACACS+ to authenticate users when they attempt to log in to the router. (The authentication servers are tried in the order specified at the [edit system tacplus-server] hierarchy level. If no TACACS+ authentication server is available, the JUNOS software will try the next authentication method listed, password. The password option also allows users that fail to authenticate with TACACS+ to log in to the router by means of UNIX password authentication.

In effect, this configuration provides a local user fallback mechanism (traditional UNIX password) when all TACACS+ servers are unavailable but does not restrict authentication to TACACS+ authentication only (all users will be able to try traditional UNIX password as well)

Example 2: Default to Local User Password Authentication, TACACS +

If you specify the following authentication order:

```
[edit]
system authentication-order tacplus;
```

and none of the TACACS+ servers configured at the [edit system tacplus-server] hierarchy are available, the JUNOS software will try to use the password authentication method. If a TACACS+ server is available, the JUNOS software will not try to use the password authentication method.

Example 3: Default to Local User Password Authentication, RADIUS

If you specify the following authentication order:

```
[edit]
system authentication-order radius;
```

and none of the RADIUS servers configured at the [edit system radius-server] hierarchy level are available, the JUNOS software will try to use the password authentication method. If a RADIUS server is available, the JUNOS software will not try to use the password authentication method.

Example 4: Default to Local User Password Authentication, TACACS + and RADIUS

If you specify the following authentication order:

```
[edit]  
system authentication-order [tacplus radius];
```

and no TACACS+ authentication server is available but at least one RADIUS authentication server responds (but fails to authenticate), the JUNOS software will try to use the local user fallback mechanism (password authentication method).



Note

If any one authentication method (RADIUS or TACACS+) fails to communicate with all of its configured servers, the JUNOS software will use the local user fallback mechanism (password authentication method).

Chapter 21

Configure User Access

To configure user access, you do the following:

- Define Login Classes on page 253
- Configure User Accounts on page 262

For information about how to configure user access through ssh, see “Configure ssh Service” on page 281.

Define Login Classes

All users who can log into the router must be in a login class. With login classes, you define the following:

- Access privileges users have when they are logged into the router
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged off

You can define any number of login classes. You then apply one login class to an individual user account, as described in “Configure User Accounts” on page 262.

To define a login class and its access privileges, include the class statement at the [edit system login] hierarchy level:

```
[edit system]
login {
  class class-name {
    allow-commands "regular-expression";
    allow-configuration "regular-expression";
    deny-commands "regular-expression";
    deny-configuration "regular-expression";
    idle-timeout minutes;
    permissions [ permissions ];
  }
}
```

Use *class-name* to name the login class. The software contains a few predefined login classes, which are listed in Table 11, “Default System Login Classes” on page 256. The predefined login classes cannot be modified.

**Note**

You cannot modify a predefined login class name. If you issue the set command on a predefined class name, the JUNOS software will append -local to the login class name. The following message also appears:

warning: '<classname>' is a predefined class name;
changing to '<classname> -local'

**Note**

You cannot issue the rename or copy command on a predefined login class. Doing so results in the following error message:

error: target '<classname>' is a predefined class

For each login class, you can do the following:

- Configure Access Privilege Levels on page 254
- Deny or Allow Individual Commands on page 256
- Configure the Timeout Value for Idle Login Sessions on page 262

Configure Access Privilege Levels

Each top-level CLI command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The privilege level for each command and statement is listed in the summary chapter of the part in which that command or statement is described. The access privileges for each login class are defined by one or more *permission bits*.

To configure access privilege levels, include the permissions statement at the [edit system login class] hierarchy level:

```
[edit system login class]
permissions [ permissions ];
```

In *permissions*, specify one or more of the permission bits listed in Table 10. Permission bits are not cumulative, so for each class list all the bits needed, including view to display information and configure to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- “Plain” form—Provides read-only capability for that permission type. An example is interface.
- Form that ends in -control—Provides read and write capability for that permission type. An example is interface-control.

Table 10: Login Class Permission Bits

Permission Bit	Description
admin	Can view user account information in configuration mode and with the show configuration command.
admin-control	Can view user accounts and configure them (at the [edit system login] hierarchy level).
access	Can view the access configuration in configuration mode and with the show configuration operational mode command.
access-control	Can view and configure access information (at the [edit access] hierarchy level).
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands).
configure	Can enter configuration mode (using the configure command) and commit configurations (using the commit command).
control	Can perform all control-level operations (all operations configured with the -control permission bits).
edit	Can edit all portions of a configuration, can load a configuration from an ASCII file, and can commit new and modified configurations (using all the commands in configuration mode).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the [edit firewall] hierarchy level).
floppy	Can read from and write to the removable media.
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	Can view interface configuration information and configure interfaces (at the [edit interfaces] hierarchy level).
maintenance	Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the router (using the request system commands).
network	Can access the network by entering the ping, ssh, telnet, and traceroute commands.
reset	Can restart software processes using the restart command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level).
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
shell	Can start a local shell on the router by entering the start shell command.
snmp	Can view SNMP configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).

Permission Bit	Description
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the [edit system] hierarchy level).
trace	Can view trace file settings in configuration and operational modes.
trace-control	Can view trace file settings and configure trace file properties.
view	Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics.

Table 11: Default System Login Classes

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
super-user	all
unauthorized	None

Example: Configure Access Privilege Levels

Create two access privilege classes on the router, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

```
[edit]
system {
  login {
    class user-accounts {
      permissions [ configure admin admin-control ];
    }
    class network-mgmt {
      permissions [ configure snmp snmp-control ];
    }
  }
}
```

Deny or Allow Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the permissions statement. For information about CLI commands, see “Command-Line Interface Overview” on page 101.



Note

The all login class permission bits take precedence over extended regular expressions when a user issues the rollback command.

Users cannot issue the load override command when specifying an extended regular expression. Users can only issue the merge, replace, and patch configuration commands.

This section describes how to define a user's access privileges to individual operational and configuration mode commands. It contains the following topics:

- Operational Mode Commands on page 257
- Configuration Mode Commands on page 259

Operational Mode Commands

You can specify extended regular expressions with the `allow-commands` and `deny-commands` attributes to define a user's access privileges to individual operational commands. Doing so takes precedence over login class permission bits set for a user. You can include one `deny-commands` and one `allow-commands` statement in each login class.

To explicitly allow an individual operational mode command that would otherwise be denied, include the `allow-commands` statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
  allow-commands "regular-expression";
```

To explicitly deny an individual operational mode command that would otherwise be allowed, include the `deny-commands` statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
  deny-commands "regular-expression";
```

If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Regular expressions are not case-sensitive.

Use extended regular expressions to specify which operational mode commands are denied or allowed. You specify these regular expressions in the `allow-commands` and `deny-commands` statements at the [edit system login class] hierarchy level, or by specifying JUNOS-specific attributes in your TACACS+ or RADIUS authentication server's configuration. You must specify that these regular expressions are sent as the value of Juniper vendor-specific attributes. If regular expressions are received during TACACS+ or RADIUS authentication, they override any regular expressions configured on the local router. For information about TACACS+ or RADIUS authentication, see "Configure User Access" on page 253.

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 12 lists common regular expression operators.

Table 12: Operational Mode Commands—Common Regular Expression Operators

Operator	Match...
	One of the two terms on either side of the pipe.
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces \$" means that the user cannot issue show interfaces detail or show interfaces extensive.
[]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
()	A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression.

If a regular expression contains a syntax error, authentication fails and the user cannot log in. If a regular expression does not contain any operators, all varieties of the command are allowed. For example, if the following statement is included in the configuration, the user can issue the commands show interfaces detail and show interfaces extensive in addition to showing an individual interface:

```
allow-commands "show interfaces"
```

Example 1: Define Access Privileges to Individual Operational Mode Commands

The following examples define user access privileges to individual operational mode commands.

If the following statement is included in the configuration and the user does not have the configure login class permission bit, the user can enter configuration mode

```
[edit system login class class-name]
user@host# set allow-commands configure
```

If the following statement is included in the configuration and the user does not have the configure login class permission bit, the user can enter configuration exclusive mode.

```
[edit system login class class-name]
user@host# set allow-commands "configure exclusive"
```



Note

You cannot use runtime variables. In the following example the runtime variable 1.2.3.4 cannot be used.

```
[edit system login class class-name]
user@host set deny "show bgp neighbor 1.2.3.4"
```

Example 2: Define Access Privileges to Individual Operational Mode Commands

Configure permissions for individual operational mode commands:

```
[edit]
system {
  login {
    /*
    * This login class has operator privileges and the additional ability to reboot the router.
    */
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    /*
    * This login class has operator privileges but can't use any commands beginning with "set".
    */
    class operator-no-set {
      permissions [ clear network reset trace view ];
      deny-commands "^set";
    }
    /*
    * This login class has operator privileges and can install software but not view bgp
    information.
    */
    class operator-and-install-but-no-bgp {
      permissions [ clear network reset trace view ];
      allow-commands "request system software add";
      deny-commands "show bgp";
    }
  }
}
```

Configuration Mode Commands

You can specify extended regular expressions with the `allow-configuration` and `deny-configuration` attributes to define user access privileges to parts of the configuration hierarchy or individual configuration mode commands. Doing so overrides login class permission bits set for a user. You can also use wildcards to restrict access. When you define access privileges to parts of the configuration hierarchy or individual configuration mode commands, do the following:

- Specify the full paths in the extended regular expressions with the `allow-configuration` and `deny-configuration` attributes.
- Enclose parentheses around an extended regular expression that connects two or more terms with the pipe (`|`) symbol. For example:

```
[edit system login class class-name]
user@host# set deny-configuration "(system login class)|(system services)"
```



Note

Do not use spaces between regular expressions separated with parentheses and connected with the pipe (`|`) symbol.

You cannot define access to keywords such as `set`, `edit`, or `activate`.

For more information about how to use wildcards, see Table 13, “Configuration Mode Commands—Common Regular Expression Operators” on page 260.

To explicitly allow an individual configuration mode command that would otherwise be denied, include the allow-configuration statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
  allow-configuration "regular-expression";
```

To explicitly deny an individual configuration mode command that would otherwise be allowed, include the deny-configuration statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
  deny-configuration "regular-expression";
```

If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Regular expressions are not case-sensitive.

You can include one deny-configuration and one allow-configuration statement in each login class.

Use extended regular expressions to specify which configuration mode commands are denied or allowed. You specify these regular expressions in the allow-configuration and deny-configuration statements at the [edit system login class] hierarchy level, or by specifying JUNOS-specific attributes in your TACACS+ or RADIUS authentication server's configuration. You must specify that these regular expressions are sent as the value of Juniper vendor-specify attributes. If regular expressions are received during TACACS+ or RADIUS authentication, they override any regular expressions configured on the local router. For information about TACACS+ or RADIUS authentication, see “Configure User Access” on page 253.

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2. Table 13 lists common regular expression operators.

Table 13: Configuration Mode Commands—Common Regular Expression Operators

Operator	Match...
	One of the two terms on either side of the pipe.
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces \$" means that the user cannot issue show interfaces detail or show interfaces extensive.
[]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
()	A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression.
*	0 or more terms.
+	One or more terms.
.	Any character except for a space " " .

Example 3: Define Access Privileges to Individual Configuration Mode Commands

The following examples show how to configure access privileges to individual configuration mode commands.

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@host# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot issue login class commands within any login class whose name begins with "m".

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m.*"
```

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot issue configuration mode commands at the login class or system services hierarchy levels.

```
[edit system login class class-name]
user@host# set deny-configuration "(system login class) | (system services)"
```

If the following statement is included in the configuration and the user's login class permission bit is set to protocols, the user cannot issue login class commands within any login class whose name begins with "m".

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m.*"
```

Example 4: Configure Access Privileges to Individual Configuration Mode Commands

Configure permissions for individual configuration mode commands:

```
[edit]
system {
  login {
    /*
     * This login class has operator privileges and the additional ability to issue commands at the
     * system services hierarchy.
     */
    class only-system-services {
      permissions [ configure ];
      allow-configuration "system services";
    }
    /*
     * This login class has operator privileges but can't issue any system services commands.
     */
    class all-except-system-services {
      permissions [ all ];
      deny-configuration "system services";
    }
  }
}
```

Configure the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router, even if that session is idle. To close idle sessions automatically, you configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

To define the timeout value for idle login sessions, include the `idle-timeout` statement at the `[edit system login class]` hierarchy level:

```
[edit system login class class-name]  
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.

```
user@host# Session will be closed in 5 minutes if there is no activity.  
Warning: session will be closed in 1 minute if there is no activity  
Warning: session will be closed in 10 seconds if there is no activity  
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed except if the user is running Telnet or monitoring interfaces using the `monitor interface` or `monitor traffic` command.

Configure User Accounts

User accounts provide one way for users to access the router. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers, as described in “User Authentication” on page 227.) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

To create user accounts, include the `user` statement at the `[edit system login]` hierarchy level:

```
[edit system]  
login {  
  user user-name {  
    full-name complete-name;  
    uid uid-value;  
    class class-name;  
    authentication {  
      (encrypted-password "password" | plain-text-password);  
      ssh-rsa "public-key";  
      ssh-dsa "public-key";  
    }  
  }  
}
```

For each user account, you can define the following:

- **User name**—(Optional) Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the user name.
- **User's full name**—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
- **User identifier (UID)**—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range 100 through 64000 and must be unique within the router. If you do not assign a UID to a user name, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration, then assigns the duplicate UID.

- **User's access privilege**—(Required) One of the login classes you defined in the class statement at the [edit system login] hierarchy level or one of the default classes listed in Table 11, "Default System Login Classes" on page 256.
- **Authentication method or methods and passwords** that the user can use to access the router—(Optional) You can use ssh or an MD5 password, or you can enter a plain-text password that the JUNOS software encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the plain-text-password option, you are prompted to enter and confirm the password:

```
[edit system]
user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

For ssh authentication, you can copy the contents of an ssh keys file into the configuration. For information about how to specify filenames, see "How to Specify Filenames and URLs" on page 224.

To load an ssh key file, use the load-key-file command. This command loads RSA (ssh version 1) and DSA (ssh version 2) public keys. You can also configure a user to use ssh-rsa and ssh-dsa keys.

If you load the ssh keys file, the contents of the file are copied into the configuration immediately after you enter the load-key-file statement. To view the ssh keys entries, use the configuration mode show command. For example:

```
[edit system]
user@host# set root-authentication load-key-file my-host::ssh/identity.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
  ssh-rsa "1024 35 97276382040842510554682267572498642416303222074049625
2839038203869014158453496417001961060835872296156347578491827360336
1276441874265946893207739108344810126831259577226254616679992783161
2350043866091586628382248974673260566119218148953981396556156378621
194032768780653816960202749164163735913269396344008443
boojum@juniper.net"; # SECRET-DATA
}
```

An account for the user root is always present in the configuration. You configure the password for root using the root-authentication statement, as described in “Configure the Root Password” on page 239.

Example: Configure User Accounts

Create accounts for four router users, and create an account for the template user “remote.” All users use one of the default system login classes.

```
[edit]
system {
  login {
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class superuser;
      authentication {
        encrypted-password "$1$poPpeY";
      }
    }
    user alexander {
      full-name "Alexander the Great";
      uid 1002;
      class view;
      authentication {
        encrypted-password "$1$14c5.$sBopasdFFdssdFFdsdfs0";
        ssh-dsa "8924 37 5678 5678@gaugamela.per";
      }
    }
    user darius {
      full-name "Darius King of Persia";
      uid 1003;
      class operator;
      authentication {
        ssh-rsa "1024 37 12341234@ecbatana.per";
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Chapter 22

Configure Time

This chapter discusses the following topics related to configuring time:

- Set the Time Zone on page 265
- Configure the Network Time Protocol on page 266

For more information about configuring time, see “Set the Current Date and Time” on page 119. For more information about setting the date and time for NTP servers, see “Set Date and Time from NTP Servers” on page 119.

Set the Time Zone

The default local time zone on the router is UTC (Coordinated Universal Time, formerly known as Greenwich Mean Time). To modify the local time zone, include the `time-zone` statement at the `[edit system]` hierarchy level:

```
[edit system]
time-zone time-zone;
```

You specify the *time-zone* using the continent/country/zone primary name. For the time zone change to take effect for all processes running on the router, you must reboot the router.

For information about setting the time on the router, see “Set the Current Date and Time” on page 119.

Examples: Set the Time Zone

Set the time zone for New York:

```
[edit]
user@host# set system time-zone America/New_York
[edit]
user@host# show
system {
    time-zone America/New_York;
}
```

Set the time zone for Pacific Time:

```
[edit]
user@host# set system time-zone America/Los_Angeles
[edit]
user@host# show
system {
    time-zone America/Los_Angeles;
}
```

For information about what time zones are available, see “time-zone” on page 315.

Configure the Network Time Protocol

The Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network. NTP uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical master-slave configuration synchronizes local clocks within the subnet and to national time standards by means of wire or radio. The servers also can redistribute reference time using local routing algorithms and time daemons.

NTP is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

To configure NTP on the router, include the `ntp` statement at the [edit system] hierarchy level:

```
[edit system]
ntp {
    authentication-key number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}
```

To configure NTP properties, you can do one or more of the following:

- Configure the NTP Boot Server on page 267
- Configure the NTP Time Server and Time Services on page 267
- Configure NTP Authentication Keys on page 269
- Configure the Router to Listen for Broadcast Messages on page 270
- Configure the Router to Listen for Multicast Messages on page 270

When configuring NTP, you do not actively configure time servers. Rather, all clients also are servers. An NTP server is not believed unless it, in turn, is synchronized to another NTP server—which itself must be synchronized to something upstream, eventually terminating in a high-precision clock.

If the time difference between the local router clock and the NTP server clock is more than 128 milliseconds, but less than 128 seconds, the clocks are slowly stepped into synchronization. However, if the difference is more than 128 seconds, the clocks are not synchronized. You must set the time on the local router so that the difference is less than 128 seconds to start the synchronization process. On the local router, you set the date and time using the `set date` command. To set the time automatically, use the `boot-server` statement at the `[edit system ntp]` hierarchy level, specifying the address of an NTP server.

Configure the NTP Boot Server

When you boot the router, it issues an `ntpdate` request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's time.

To configure the NTP boot server, include the `boot-server` statement at the `[edit system ntp]` hierarchy level:

```
[edit system ntp]
boot-server address;
```

Specify the address of the network server. You must specify an address, not a hostname.

Configure the NTP Time Server and Time Services

When configuring NTP, you can specify which system on the network is the authoritative time source, or time server, and how time is synchronized between systems on the network. To do this, you configure the router to operate in one of the following modes:

- **Client mode**—In this mode, the local router can be synchronized to the remote system, but the remote system can never be synchronized to the local router.
- **Symmetric active mode**—In this mode, the local router and the remote system can synchronize each other. You use this mode in a network in which either the local router or the remote system might be a better source of time.



Note

Symmetric active mode can be initiated by either the local or remote system. Only one system needs to be configured to do so. This means that the local system can synchronize to any system that offers symmetric active mode without any configuration whatsoever. However, we strongly encourage you to configure authentication to ensure that the local system synchronizes only to known time servers.

- **Broadcast mode**—In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast *address*. Normally, you include this statement only when the local router is operating as a transmitter.

The following sections describe how to configure these modes of operation:

- Configure the Router to Operate in Client Mode on page 268
- Configure the Router to Operate in Symmetric Active Mode on page 268
- Configure the Router to Operate in Broadcast Mode on page 269

Configure the Router to Operate in Client Mode

To configure the local router to operate in client mode, include the server statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
server address <key key-number> <version value> <prefer>;
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in “Configure NTP Authentication Keys” on page 269.

By default, the router sends NTP version 3 packets to the time server. To set the NTP version level to 1 or 2, include the version option.

If you configure more than one time server, you can mark one server as being preferred by including the prefer option.

Configure the Router to Operate in Symmetric Active Mode

To configure the local router to operate in symmetric active mode, include the peer statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
peer address <key key-number> <version value> <prefer>;
```

Specify the address of the remote system. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the remote system, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in “Configure NTP Authentication Keys” on page 269.

By default, the router sends NTP version 3 packets to the remote system. To set the NTP version level to 1 or 2, include the version option.

If you configure more than one remote system, you can mark one system as being preferred by including the prefer option:

```
peer address <key key-number> <version value> <prefer>;
```


Configure the Router to Operate in Broadcast Mode

To configure the local router to operate in broadcast mode, include the broadcast statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
broadcast address <key key-number> <version value> <ttl value>;
```

Specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. Currently, the multicast address must be 224.0.1.1.

To include an authentication key in all messages sent to the remote system, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in “Configure NTP Authentication Keys” on page 269.

By default, the router sends NTP version 3 packets to the remote system. To set the NTP version level to 1 or 2, include the version option.

Configure NTP Authentication Keys

Time synchronization can be authenticated to ensure that the local router obtains its time services only from known sources. By default, network time synchronization is unauthenticated. The system will synchronize to whatever system appears to have the most accurate time. We strongly encourage you to configure authentication of network time services.

To authenticate other time servers, include the trusted-key statement at the [edit system ntp] hierarchy level. Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible to be synchronized to. Other systems can synchronize to the local router without being authenticated.

```
[edit system ntp]
trusted-key [ key-numbers ];
```

Each key can be any 32-bit unsigned integer except 0. Include the key option in the peer, server, or broadcast statements to transmit the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize to the local system.

To define the authentication keys, include the authentication-key statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
```

number is the key number, *type* is the authentication type (either MD5 or DES), and *password* is the password for this key. The key number, type, and password must match on all systems using that particular key for authentication.

Configure the Router to Listen for Broadcast Messages

When you are using NTP, you can configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet by including the `broadcast-client` statement at the `[edit system ntp]` hierarchy level:

```
[edit system ntp]
broadcast-client;
```

When the router hears a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. Then, it enters *broadcast client* mode, in which it listens for, and synchronizes to, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

Configure the Router to Listen for Multicast Messages

When you are using NTP, you can configure the local router to listen for multicast messages on the local network to discover other servers on the same subnet by including the `multicast-client` statement at the `[edit system ntp]` hierarchy level:

```
[edit system ntp]
multicast-client <address>;
```

When the router hears a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. Then, it enters *multicast client* mode, in which it listens for, and synchronizes to, succeeding multicast messages.

You can specify one or more IP addresses. (You must specify an address, not a hostname.) If you do, the route joins those multicast groups. If you do not specify any addresses, the software uses 224.0.1.1.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

Chapter 23

Configure System Logging

The chapter discusses the following topics:

- Configure System Logging on page 271
- Archive System Logs on page 273
- Override the Facility on page 274
- Configure Log Message Prefixes on page 275

Go to page 275 for system logging configuration examples.

Configure System Logging

System logging operations use a system logging mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging in to or out of the router.

To control system logging and how much information the system should log, include the `syslog` statement at the `[edit system]` hierarchy level:

```
[edit system]
syslog {
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
  file filename {
    facility level;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
}
```

```

host hostname {
    facility level;
    facility-override facility;
    log-prefix string;
}
user (username | *) {
    facility level;
}
console {
    facility level;
}
}

```

You can log specified system information to one or more destinations. The destinations can be one or more files, one or more remote hosts, the terminals of one or more users who are logged in, and the system console.

For each place where you can log system information, you specify the class (*facility*) of messages to log and the minimum severity level (*level*) of the message.

Table 14 lists the system logging facilities, and Table 15 lists the system logging severity levels.

Table 14: System Logging Facilities

Facility	Description
any	Any facility
authorization	Any authorization attempt
change-log	Any change to the configuration
conflict-log	Messages generated when configuration conflicts with hardware
cron	Cron daemon
daemon	Various system daemons
firewall	Firewall filtering subsystem
interactive-commands	Commands executed in the CLI
kernel	Messages generated by the JUNOS kernel
pfe	Messages generated by the packet forwarding engine (pfe)
user	Messages from random user processes

Table 15: System Logging Severity Levels

Severity Level (from Highest to Lowest Severity)	Description
emergency	Panic or other conditions that cause the system to become unusable.
alert	Conditions that should be corrected immediately, such as a corrupted system database.
critical	Critical conditions, such as hard drive errors.
error	Standard error conditions.
warning	System warning messages.
notice	Conditions that are not error conditions, but that might warrant special handling.
info	Informational messages. This is the default.
debug	Software debugging messages.

A common set of operations to log is when users log into the router and when they issue CLI commands. To configure this type of logging, specify the interactive-commands facility and one of the following severity levels:

- info—Log all top-level CLI commands, including the configure command, and all configuration mode commands.
- notice—Log the configuration mode commands rollback and commit.
- warning—Log when any software process restarts.

Another common operation to log is when users enter authentication information. To configure this type of logging, specify the authorization facility.

Archive System Logs

Logging information is saved to one or more files. By default, the software stores the logging information in up to ten 128-KB files, and by default, these files can be read by a limited group of users. To modify the number and size of all system log files, as well as who can read them, include the archive option at the [edit system syslog] hierarchy level:

```
[edit system]
syslog {
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
}
```

To modify the number and size of a particular system log file, as well as who can read it, include the archive option at the [edit system syslog file *filename*] hierarchy level:

```
[edit system]
syslog {
  file filename {
    facility level;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
}
```

You can configure any number of files in the range 1 through 1000, and they can be any size in the range 64 KB (64k) through 1 GB (1g).

To allow any user to read the log file, include the world-readable option.

Override the Facility

When sending messages to a remote host, you can override the facility. For example, you can configure all messages from a single router to go to a single log file on the remote host. You can also configure different routers to send messages to different log files on the same remote host to, for example, segregate messages representing different regions of the country.

To override the facility, include the facility-override statement at the [edit system syslog host *hostname*] hierarchy level.

```
[edit system syslog host hostname]
facility-override facility;
```

Table 16 lists the system logging facilities that you can specify on the facility-override statement.

Table 16: System Logging Facilities That You Can Specify on the facility-override Statement

Facility	Description
authorization	Any authorization attempt
cron	Cron daemon
daemon	Various system daemons
kernel	Messages generated by the JUNOS kernel
local0	Local logging option number 0
local1	Local logging option number 1
local2	Local logging option number 2
local3	Local logging option number 3
local4	Local logging option number 4

Facility	Description
local5	Local logging option number 5
local6	Local logging option number 6
local7	Local logging option number 7
user	Messages from random user processes

Configure Log Message Prefixes

You can configure a string to be prepended to every log message sent to the remote host, which is useful for identifying the router from which it came. The string cannot contain spaces, equal signs (=), or colons (:). To prepend a string to log messages sent to a remote host, include the log-prefix statement at the [edit system syslog host *hostname*] hierarchy level.

```
[edit system syslog host hostname]
log-prefix string;
```

A colon and a space are appended to the string when the syslog messages are written to the log. For example, if the string is configured as JNPR:

```
Mar 9 17:33:23 host JNPR: mgd[477]: UI_CMDLINE_READ_LINE: user 'root', command 'run show
version'
```

Examples: Configure System Logging

Log system logging information to two files, one remote host (the user Alex's terminal), and the system console:

```
[edit system]
syslog {
  /* send all security-related information to file "security" */
  file security {
    authorization info;
    interactive-commands info;
  }
  /* send generic messages (authorization at level notice and above,
  the rest at level warning and above) to file "messages" */
  file messages {
    authorization notice;
    any warning;
  }
  /* send any critical messages to alex if he is logged in */
  user alex {
    any critical;
  }
  /* send all daemon level info and above, or anything warning and above, to
  the host junipero.berry.net */
  host junipero.berry.net {
    daemon info;
    any warning;
  }
  /* send any error messages, or higher, to the system console */
  console {
    any error;
  }
}
```

Log all CLI commands entered by all users and all authorization attempts to a file and to the terminals of all users who are logged in:

```
[edit system]
syslog {
  file cli-commands {
    interactive-commands info;
    authorization info;
  }
  user * {
    interactive-commands info;
    authorization info;
  }
}
```

Log all CLI commands entered by any user to the user Philip's terminal and log only the rollback and commit commands entered by any user to the user Darius' terminal:

```
[edit system]
syslog {
  user philip {
    interactive-commands any;
  }
  user darius {
    any notice;
  }
}
```

Log the changing of alarms:

```
[edit system]
syslog {
  file alarms {
    daemon warning;
  }
}
```


Chapter 24

Configure Miscellaneous System Management Features

This chapter discusses the following topics:

- Configure Console and Auxiliary Port Properties on page 277
- Disable the Sending of Redirect Messages on the Router on page 278
- Configure the Source Address for Locally Generated TCP/IP Packets on page 278
- Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent on page 279
- Configure System Services on page 280
- Configure a System Login Message on page 283
- Configure JUNOS Software Processes on page 283
- Configure a Password on the Diagnostics Port on page 284
- Core Dump Files on page 284

Configure Console and Auxiliary Port Properties

The router's craft interface has two ports—a console port and an auxiliary port—for connecting terminals to the router. The console port is enabled by default, and its speed is 9600 baud. The auxiliary port is disabled by default.

To configure the properties for the console and auxiliary ports, include the ports statement at the [edit system] hierarchy level:

```
[edit system]
ports {
  auxiliary {
    type terminal-type;
  }
  console {
    type terminal-type;
  }
}
```

By default, the terminal type is unknown, and the terminal speed is 9600 baud for both the console and auxiliary ports. To change the terminal type, include the `type` statement, specifying a *terminal-type* of `ansi`, `vt100`, `small-xterm`, or `xterm`. The first three terminal types set a screen size of 80 columns by 24 lines. The last type, `xterm`, sets the size to 80 columns by 65 rows.

By default, terminal connections to the console and auxiliary ports are secure. That is, it is safe to log in as root and enter the root password.

Disable the Sending of Redirect Messages on the Router

By default, the router sends protocol redirect messages. To disable the sending of redirect messages by the router, include the `no-redirects` statement at the `[edit system]` hierarchy level:

```
[edit system]
no-redirects;
```

To re-enable the sending of redirect messages on the router, delete the `no-redirects` statement from the configuration.

To disable the sending of redirect messages on a per-interface basis, include the `no-redirects` statement at the `[edit interfaces interface-name unit logical-unit-number family family]` hierarchy level as described in the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Configure the Source Address for Locally Generated TCP/IP Packets

By default, the source address included in locally generated TCP/IP packets, such as FTP traffic, and in UDP and IP packets, such as NTP requests, is chosen as the local address for the interface on which the traffic is transmitted. This means that the local address chosen for packets to a particular destination might change from connection to connection based on the interface that the routing protocol has chosen to reach the destination when the connection is established.

To configure the software to select a fixed address to use as the source for locally generated IP packets, include the `default-address-selection` statement at the `[edit system]` hierarchy level:

```
[edit system]
default-address-selection;
```

If you include the `default-address-selection` statement in the configuration, the software chooses the system default address as the source for most locally generated IP packets. The default address is usually an address configured on the `lo0` loopback interface. For example, if you specified that `ssh` and `Telnet` use a particular address, but you also have `default-address-selection` configured, the system default address is used. For more information about how the default address is chosen, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

For IP packets sent by IP routing protocols (including OSPF, RIP, RSVP, and the multicast protocols, but not including IS-IS), the local address selection is often constrained by the protocol specification so that the protocol operates correctly. When this constraint exists in the routing protocol, the packet's source address is unaffected by the presence of the default-address-selection statement in the configuration. For protocols in which the local address is unconstrained by the protocol specification, for example, IBGP and multihop EBGp, if you do not configure a specific local address when configuring the protocol, the local address is chosen using the same method as other locally generated IP packets.

Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent

You can configure the router or an interface to act as a Dynamic Host Configuration Protocol (DHCP) or BOOTP relay agent. This means that a locally attached host can issue a DHCP or BOOTP request as a broadcast message. If the router or an interface sees this broadcast message, it relays the message to a specified DHCP or BOOTP server.

You should configure the router or an interface to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

To configure the router to act as a DHCP/BOOTP relay agent, include the `dhcp-relay` statement at the `[edit system]` hierarchy level, specifying the address of the DHCP or BOOTP server:

```
[edit system]
dhcp-relay {
  no-listen;
  maximum-hop-count number;
  minimum-wait-time seconds;
  server [ address ];
  interface interface-group {
    no-listen;
    maximum-hop-count number;
    minimum-wait-time seconds;
    server [ address ];
  }
}
```



You can now configure this feature at the `[edit forwarding-options helpers bootp]` hierarchy level, which overrides the configuration at the `[edit system dhcp-relay]` hierarchy level. For more information about configuring DHCP/BOOTP relay agent at the `[edit forwarding-options helpers bootp]`, see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

`server` sets the IP address or addresses that specifies the DHCP or BOOTP server for the router or interface. You can include as many addresses as necessary in the same statement.

`no-listen` stops packets from being forwarded on a logical interface, a group of logical interfaces, or router.

`interface` sets a logical interface or a group of logical interfaces with a specific DHCP-relay or BOOTP configuration.

maximum-hop-count sets the maximum allowed number in the hops field of the BOOTP header. Headers that have a larger number in the hops field are not forwarded. If you omit the maximum-hop-count statement, the default value is 4 hops.

minimum-wait-time sets the minimum allowed number of seconds in the secs field of the BOOTP header. Headers that have a smaller number in the secs field are not forwarded. If you omit the minimum-wait-time statement, the default value is 3 seconds.

To configure an interface to act as a DHCP/BOOTP relay agent, include the interface statement at the [edit system dhcp-relay] hierarchy level, specifying the address of the DHCP or BOOTP server.



The interface statement configured under the [edit system dhcp-relay] hierarchy has the same syntax and defaults as the dhcp-relay statement. The configuration described in this section differs only in allowing you to fine-tune the router's response capabilities.

You can also configure an individual logical interface to be a DHCP/BOOTP relay if you have locally attached hosts and a remote DHCP or BOOTP server at the [edit interfaces] hierarchy level. For more information, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Configure System Services

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the finger, FTP, rlogin, ssh, and telnet services.

This section discusses the following topics:

- Configure Finger Service on page 280
- Configure FTP Service on page 281
- Configure rlogin Service on page 281
- Configure ssh Service on page 281
- Configure telnet Service on page 283

Configure Finger Service

To configure the router to accept finger as an access service, include the finger statement at the [edit system services] hierarchy level:

```
[edit system services]
  finger {
    <connection-limit limit>;
    <rate-limit limit>;
  }
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

Configure FTP Service

To configure the router to accept the FTP as an access service, include the `ftp` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
ftp {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

Configure rlogin Service

To configure the router to accept rlogin as an access service, include the `rlogin` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
rlogin {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

Configure ssh Service

To configure the router to accept ssh as an access service, include the `ssh` statement at the `[edit system services]` hierarchy level.

```
[edit system]
services {
  ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    <connection-limit limit>;
    <rate-limit limit>;
  }
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

The following sections explain how to specify the remaining options:

- [Configure Root Login on page 282](#)
- [Configure ssh Protocol Version on page 282](#)

Configure Root Login

By default, users are allowed to log in to the router as root through ssh. To control user access through ssh, include the root-login statement at the [edit system services ssh] hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

- **allow**—allows users to log in to the router as root through ssh. The default is allow.
- **deny**—disables users from logging in to the router as root through ssh.
- **deny-password**—allows users to log in to the router as root through ssh when the authentication method; for example, the RSA authentication method does not require a password.



Note

The root-login and protocol-version statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to release 5.0, the root-login and protocol-version statements are ignored if they are present in the configuration file.

Configure ssh Protocol Version

By default, version 2 of the ssh protocol is enabled. To configure the router to use version 1 only of the ssh protocol, include the protocol-version statement and specify v1 at the [edit system services ssh] hierarchy level:

```
[edit system services ssh]
protocol-version [version];
```

To configure the router to use version 1 and 2 of the ssh protocol, include the protocol-version statement and specify v1 and v2 at the [edit system services ssh] hierarchy level

```
[edit system services ssh]
protocol-version [version];
```

You can specify v1, v2, or both versions [v1 v2] of the ssh protocol. The default is v2].



Note

The root-login and protocol-version statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to release 5.0, the root-login and protocol-version statements are ignored if they are present in the configuration file.

Configure telnet Service

To configure the router to accept telnet as an access service, include the telnet statement at the [edit system services] hierarchy level:

```
[edit system services]
telnet {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

Configure a System Login Message

By default, no login message is displayed. To configure a system login message, include the message statement at the [edit system login] hierarchy level:

```
[edit system login]
message text;
```

Configure JUNOS Software Processes

By default, all JUNOS software processes are enabled on the router. To control the software processes on the router, you can do the following:

- Disable JUNOS Software Processes on page 283
- Configure Failover to Backup Media if a Software Process Fails on page 284

Disable JUNOS Software Processes



Never disable any of the software processes unless instructed to do so by a customer support engineer.

To disable a software process, specify the appropriate option in the processes statement at the [edit system] hierarchy level:

```
[edit system]
processes {
  inet-process (enable | disable);
  interface-control (enable | disable);
  mib-process (enable | disable);
  ntp (enable | disable);
  routing (enable | disable);
  snmp (enable | disable);
  watchdog (enable | disable) timeout seconds;
}
```

Configure Failover to Backup Media if a Software Process Fails

For routers with redundant Routing Engines, in the event that a software process fails repeatedly, you can configure the router to switch to backup media containing an alternate version of the system, either the alternate media or the other Routing Engine. To configure the switch to the backup media, include the failover statement at the [edit system processes *process-name*] hierarchy level:

```
[edit system processes]
  process-name failover (alternate-media | other-routing-engine);
```

process-name is one of the valid process names. If this statement is configured for a process, and that process fails three times in quick succession, the router reboots from either the alternative media or the other Routing Engine.

Configure a Password on the Diagnostics Port

If you have been asked by Customer Support personnel to connect a physical console to the router's System Control Board (SCB), System and Switch Board (SSB), or Switching and Forwarding Model (SFM) to perform diagnostics, you can configure a password on the diagnostics port. This password provides an extra level of security.

To configure a password on the diagnostics port, include the diag-port-authentication statement at the [edit system] hierarchy level:

```
[edit system]
  diag-port-authentication (encrypted-password "password" | plain-text-password);
```

You can use an MD5 password, or you can enter a plain-text password that the JUNOS software encrypts (using MD5-style encryption) before it places it into the password database. For an MD5 password, specify the password in the configuration. If you configure the plain-text-password option, the CLI prompts you for the password.

For routers that have more than one SSB, the same password is used for both SSBs.

Core Dump Files

By default, core files generated by internal JUNOS processes are now saved along with contextual information in compressed tar files stored under `/var/tmp/process-name.core.core-number.tgz` for debugging purposes. The contextual information contains the configuration and log messages file.

To turn this feature off, include the no-saved-core-context statement at the [edit system] hierarchy level.

```
[edit system]
  user@host# set no-saved-core-context
```


Chapter 25

Summary of System Management Configuration Statements

The following sections explain each of the system management configuration statements. The statements are organized alphabetically.

allow-commands

Syntax	<code>allow-commands "regular-expression";</code>
Hierarchy Level	[edit system login class]
Description	Specify the operational mode commands that members of a login class can use.
Default	If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Usage Guidelines	See “Deny or Allow Individual Commands” on page 256.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	deny-commands on page 292, user on page 318

allow-configuration

Syntax	allow-configuration" <i>regular-expression</i> " ;
Hierarchy Level	[edit system login class]
Description	Specify the configuration mode commands that members of a login class can use.
Default	If you omit this statement and the deny-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Usage Guidelines	See “Deny or Allow Individual Commands” on page 256.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	deny-commands on page 292, user on page 318

authentication

Syntax	authentication { (encrypted-password " <i>password</i> " plain-text-password); ssh-rsa " <i>public-key</i> "; ssh-dsa " <i>public-key</i> "; }
Hierarchy Level	[edit system login user]
Description	Authentication methods that a user can use to log into the router. You can assign multiple authentication methods to a single user.
Options	encrypted-password " <i>password</i> "—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user. plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user. ssh-rsa " <i>public-key</i> "—Secure shell (ssh version 1) authentication. Specify the ssh public key. You can specify one or more public keys for each user. ssh-dsa " <i>public-key</i> "—Secure shell (ssh version 2) authentication. Specify the ssh public key. You can specify one or more public keys for each user.
Usage Guidelines	See “Configure User Accounts” on page 262.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	root-authentication on page 307

authentication-key

Syntax	<code>authentication-key <i>key-number</i> <i>type</i> <i>type</i> <i>value</i> <i>password</i>;</code>
Hierarchy Level	[edit system ntp]
Description	<p>Configure NTP authentication keys so that the router can send authenticated packets. If you configure the router to operate in authenticated mode, you must configure a key.</p> <p>Both the keys and the authentication schemes (DES or MD5) must be identical between a set of peers sharing the same key number.</p>
Options	<p><i>key-number</i>—Positive integer that identifies the key.</p> <p><i>type</i>—Authentication type. It can be either md5 or des.</p> <p><i>value password</i>—The key itself, which can be 1 to 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</p>
Usage Guidelines	See “Configure NTP Authentication Keys” on page 269.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
See Also	broadcast on page 289, peer on page 303, server on page 309, trusted-key on page 317

authentication-order

Syntax	<code>authentication-order [<i>authentication-methods</i>];</code>
Hierarchy Level	[edit system]
Description	Configure the order in which the software tries different user-authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
Default	If you do not include the authentication-order statement, users are verified based on their configured passwords.
Options	<p><i>authentication-methods</i>—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:</p> <ul style="list-style-type: none"> ■ password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level. ■ radius—Verify the user using RADIUS authentication services. ■ tacplus—Verify the user using TACACS+ authentication services.
Usage Guidelines	See “Configure the Authentication Order” on page 248.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

auxiliary

Syntax	auxiliary { type <i>terminal-type</i> ; }
Hierarchy Level	[edit system ports]
Description	Configure the characteristics of the auxiliary port, which is on the router's craft interface.
Default	The auxiliary port is disabled.
Options	type <i>terminal-type</i> —Type of terminal that is connected to the port. Values: ansi, vt100, small-xterm, xterm Default: The terminal type is unknown, and the user is prompted for the terminal type.
Usage Guidelines	See "Configure Console and Auxiliary Port Properties" on page 277.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

backup-router

Syntax	backup-router <i>address</i> <destination <i>destination-address</i> >;
Hierarchy Level	[edit system]
Description	Set a default router to use while the local router is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.
Options	<i>address</i> —Address of the default router. <i>destination destination-address</i> —(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table. Default: All hosts (default route) are reachable through the backup router.
Usage Guidelines	See "Configure a Backup Router" on page 237.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

boot-server

Syntax	<code>boot-server address;</code>
Hierarchy Level	[edit system ntp]
Description	<p>Configure the server that NTP queries when the router boots to determine the local date and time.</p> <p>When you boot the router, it issues an <code>ntpdate</code> request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's time.</p>
Options	<i>address</i> —Address of an NTP server. You must specify an address, not a hostname.
Usage Guidelines	See "Configure the NTP Boot Server" on page 267.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

broadcast

Syntax	<code>broadcast address <key key-number <version value> <ttl value> ;</code>
Hierarchy Level	[edit system ntp]
Description	<p>Configure the local router to operate in broadcast mode with the remote system at the specified <i>address</i>. In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast <i>address</i>. Normally, you include this statement only when the local router is operating as a transmitter.</p>
Options	<p><i>address</i>—Address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. Currently, the multicast address must be 224.0.1.1.</p> <p><i>key key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. Values: Any unsigned 32-bit integer</p> <p><i>ttl value</i>—(Optional) Time-To-Live (TTL) value to use. Range: 1 through 255 Default: 1</p> <p><i>version value</i>—(Optional) Specify the version number to be used in outgoing NTP packets. Values: 1, 2, 3 Default: 3</p>
Usage Guidelines	See "Configure the NTP Time Server and Time Services" on page 267.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

• broadcast-client

Syntax	broadcast-client;
Hierarchy Level	[edit system ntp]
Description	Configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet.
Usage Guidelines	See “Configure the Router to Listen for Broadcast Messages” on page 270.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

• class

Syntax	class <i>class-name</i> { allow-commands " <i>regular-expression</i> "; deny-commands " <i>regular-expression</i> "; idle-timeout <i>minutes</i> ; permissions [<i>permissions</i>]; }
Hierarchy Level	[edit system login]
Description	Define login classes.
Options	<i>class-name</i> —A name you choose for the login class. The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Define Login Classes” on page 253.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	user on page 318
Syntax	class <i>class-name</i> ;
Hierarchy Level	[edit system login user]
Description	Configure a user’s login class. You must configure one class for each user.
Options	<i>class-name</i> —One of the classes defined at the [edit system login class] hierarchy level.
Usage Guidelines	See “Configure User Accounts” on page 262.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

compress-configuration-files

Syntax	compress-configuration-files;
Hierarchy Level	[edit system]
Description	Compress the current operational configuration file. By default, the current operational configuration file is uncompressed, and is stored in the file <code>juniper.conf</code> , in the <code>/config</code> file system, along with the last three committed versions of the configuration. However, with large networks, the current configuration file might exceed the available space in the <code>/config</code> file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. The current configuration file is compressed on the second commit of the configuration after the first commit is made to include the <code>compress-configuration-files</code> statement.
Default	The current operational configuration file is uncompressed.
Usage Guidelines	See “Compress the Current Configuration File” on page 240.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

console

Syntax	console { type <i>terminal-type</i> ; }
Hierarchy Level	[edit system ports]
Description	Configure the characteristics of the console port, which is on the router’s craft interface.
Default	The console port is enabled and its speed is 9600 baud.
Options	type <i>terminal-type</i> —Type of terminal that is connected to the port. Values: ansi, vt100, small-xterm, xterm Default: The terminal type is unknown, and the user is prompted for the terminal type.
Usage Guidelines	See “Configure Console and Auxiliary Port Properties” on page 277.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

default-address-selection

Syntax	default-address-selection;
Hierarchy Level	[edit system]
Description	Use the loopback interface, lo0, as the source address for all locally generated IP packets. The lo0 interface is the interface to the router's Routing Engine.
Default	The outgoing interface is used as the source address.
Usage Guidelines	See "Configure the Source Address for Locally Generated TCP/IP Packets" on page 278 and the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

deny-commands

Syntax	deny-commands " <i>regular-expression</i> ";
Hierarchy Level	[edit system login class]
Description	Specify the operational mode commands the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
Default	If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Usage Guidelines	See "Deny or Allow Individual Commands" on page 256.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	allow-commands on page 285, user on page 318

deny-configuration

Syntax	deny-configuration " <i>regular-expression</i> ";
Hierarchy Level	[edit system login class]
Description	Specify the configuration mode commands the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
Default	If you omit this statement and the allow-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Usage Guidelines	See “Deny or Allow Individual Commands” on page 256.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	allow-configuration on page 286, user on page 318

dhcp-relay

Syntax

```
dhcp-relay {
  no-listen;
  maximum-hop-count number;
  minimum-wait-time seconds;
  server [ address ];
  interface interface-group {
    no-listen;
    maximum-hop-count number;
    minimum-wait-time seconds;
    server [ address ];
  }
}
```



Note

You can now configure this feature at the [edit forwarding-options helpers bootp] hierarchy level, which overrides the configuration at the [edit system dhcp-relay] hierarchy level. For more information about configuring DHCP/BOOTP relay agent at the [edit forwarding-options helpers bootp], see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

Hierarchy Level [edit system],
[edit system dhcp-relay]

Description Configures a router or interface to act as a Dynamic Host Configuration Protocol (DHCP) or BOOTP relay agent.

Default DHCP relaying is disabled.

Options no-listen—Stops packets from being forwarded on a logical interface, a group of logical interfaces, or router.

maximum-hop-count *number*—In the hops field of the BOOTP header, the maximum number of hops allowed.

Default: 4 hops

minimum-wait-time *seconds*—In the secs field of the BOOTP header, the minimum time allowed.

Default: 3 seconds


server [*address*]—Sets the IP address or addresses that specify the DHCP server or BOOTP server for the router or interface.

interface *interface-group*—Sets a logical interface or group of logical interfaces with a specific DHCP relay configuration.

Usage Guidelines See “Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent” on page 279.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

diag-port-authentication

Syntax	diag-port-authentication (encrypted-password " <i>password</i> " plain-text-password);
Hierarchy Level	[edit system]
Description	<p>Configure a password for performing diagnostics on the router's System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) port.</p> <p>For routers that have more than one SSB, the same password is used for both SSBs.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;">  <p>Note Do not run diagnostics on the SCB, SSB, SFM, or FEB unless you have been instructed to do so by customer support personnel.</p> </div>
Default	No password is configured on the diagnostics port.
Options	<p>encrypted-password "<i>password</i>"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.</p> <p>plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user.</p>
Usage Guidelines	See "Configure a Password on the Diagnostics Port" on page 284.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

domain-name

Syntax	domain-name <i>domain-name</i> ;
Hierarchy Level	[edit system]
Description	Configure the name of the domain in which the router is located. This is the default domain name that is appended to host names that are not fully qualified.
Options	<i>domain-name</i> —Name of the domain.
Usage Guidelines	See "Configure the Router's Domain Name" on page 235.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

domain-search

Syntax	domain-search [<i>domain-list</i>];
Hierarchy Level	[edit system]
Description	Configure a list of domains to be searched.
Options	<i>domain-list</i> —A list of domain names to search. The list can contain up to six domain names, with a total of up to 256 characters.
Usage Guidelines	See “Configure Which Domains to Search” on page 236.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

full-name

Syntax	full-name <i>complete-name</i> ;
Hierarchy Level	[edit system login user]
Description	Configure the complete name of a user.
Options	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
Usage Guidelines	See “Configure User Accounts” on page 262.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

host-name

Syntax	host-name <i>host-name</i> ;
Hierarchy Level	[edit system]
Description	Set the host name of the router.
Options	<i>host-name</i> —Name of the router.
Usage Guidelines	See “Configure the Router’s Name and Addresses” on page 233.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

idle-timeout

Syntax	idle-timeout <i>minutes</i> ;
Hierarchy Level	[edit system login class]
Description	For a login class, configure the maximum time that a session can be idle before the user is logged off the router. The session times out after remaining at the CLI operational mode prompt for the specified time.
Default	If you omit this statement, a user is never forced off the system after extended idle times.
Options	<i>minutes</i> —Maximum idle time. Range: 0 through 100,000 minutes
Usage Guidelines	See “Configure the Timeout Value for Idle Login Sessions” on page 262.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	user on page 318

interface

Syntax interface *interface-group* {
 no-listen;
 maximum-hop-count;
 minimum-wait-time *seconds*;
 server [*address*];
 }

Hierarchy Level [edit system dhcp-relay]

Description Configure the router or an interface to act as a Dynamic Host Configuration Protocol (DHCP) or BOOTP relay agent.

- Options**
- server sets the IP address or addresses that specifies the DHCP or BOOTP server for the router or interface. You can include as many addresses as necessary in the same statement.
 - no-listen stops packets from being forwarded on a logical interface, a group of logical interfaces, or router.
 - interface sets a logical interface or a group of logical interfaces with a specific DHCP-relay or BOOTP configuration
 - maximum-hop-count sets the maximum allowed number in the hops field of the BOOTP header. Headers that have a larger number in the hops field are not forwarded. If you omit the maximum-hop-count statement, the default value is 4 hops.
 - minimum-wait-time sets the minimum allowed number of seconds in the secs field of the BOOTP header. Headers that have a smaller number in the secs field are not forwarded. If you omit the minimum-wait-time statement, the default value is 3 seconds.

Usage Guidelines See “Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent” on page 279.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

load-key-file

Syntax load-key-file;

Hierarchy Level [edit system]

Description Loads RSA (ssh version 1) and DSA (ssh version 2) public keys from a file. The file is a URL containing one or more ssh keys.

Usage Guidelines See “Configure the Root Password” on page 239 and “Configure User Accounts” on page 262.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

location

Syntax	<pre>location { altitude <i>feet</i>; country-code <i>code</i>; hcoord <i>horizontal-coordinate</i>; lata <i>service-area</i>; latitude <i>degrees</i>; longitude <i>degrees</i>; npa-nxx <i>number</i>; postal-code <i>postal-code</i>; vcoord <i>vertical-coordinate</i>; }</pre>
Hierarchy Level	[edit system]
Description	Configure the system location in various formats.
Options	<p>altitude <i>feet</i>—Number of feet above sea level.</p> <p>country-code <i>code</i>—Two-letter country code.</p> <p>hcoord <i>horizontal-coordinate</i>—Bellcore Horizontal Coordinate.</p> <p>lata <i>service-area</i>—Long distance service area.</p> <p>latitude <i>degrees</i>—Latitude in degree format.</p> <p>longitude <i>degrees</i>—Longitude in degree format.</p> <p>npa-nxx <i>number</i>—First six digits of the phone number (area code and exchange).</p> <p>postal-code <i>postal-code</i>—Postal code.</p> <p>vcoord <i>vertical-coordinate</i>—Bellcore Vertical Coordinate.</p>
Usage Guidelines	See “Configure the System Location” on page 238.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

login

Syntax

```
login {
    message text;
    class class-name {
        allow-commands [ addresses ];
        deny-commands [ addresses ];
        idle-timeout minutes;
        permissions [ permissions ];
    }
    user user-name {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

Hierarchy Level [edit system]

Description Configure user access to the router.

Options The remaining statements are explained separately in this chapter.

Usage Guidelines See “Configure User Access” on page 253.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

message

Syntax message *text*;

Hierarchy Level [edit system login]

Description Configure a system login message.

Options *text*—Text of the message.

Usage Guidelines See “Configure a System Login Message” on page 283.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration

mirror-flash-on-disk

Syntax	mirror-flash-on-disk;
Hierarchy Level	[edit system]
Description	Configure the hard drive to automatically mirror the contents of the compact flash. The hard drive maintains a synchronized mirror copy of the compact-flash contents. Data written to the compact flash is simultaneously updated in the mirrored copy of the hard drive. If the flash drive fails to read data, the hard drive automatically retrieves its mirrored copy of the flash disk.

**Caution**

We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the request system snapshot command while flash disk mirroring is enabled.

**Note**

After you have enabled or disabled the mirror-flash-on-disk statement, you must reboot the router for your changes to take effect. To reboot, issue the request system reboot command.

Usage Guidelines	See “Configure Flash Disk Mirroring” on page 238.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

multicast-client

Syntax	multicast-client <address>;
Hierarchy Level	[edit system ntp]
Description	For NTP, configure the local router to listen for multicast messages on the local network to discover other servers on the same subnet.
Options	<i>address</i> —(Optional) One or more IP addresses. If you specify addresses, the router joins those multicast groups. Default: 224.0.1.1.
Usage Guidelines	See “Configure the Router to Listen for Multicast Messages” on page 270.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

name-server

Syntax	name-server { <i>address</i> ; }
Hierarchy Level	[edit system]
Description	Configure one or more DNS name servers.
Options	<i>address</i> —Address of the name server. To configure multiple name servers, include multiple <i>address</i> options.
Usage Guidelines	See “Configure a DNS Name Server” on page 236.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

no-redirects

Syntax	no-redirects;
Hierarchy Level	[edit system]
Description	Disable the sending of protocol redirect messages by the router. To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy level.
Default	The router sends redirect messages.
Usage Guidelines	See “Disable the Sending of Redirect Messages on the Router” on page 278.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
See Also	The no-redirects statement in the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .

no-saved-core-context

Syntax	no-saved-core-context;
Hierarchy Level	[edit system]
Description	Disable core files generated by internal JUNOS processes.
Default	Core files generated by internal JUNOS processes are now saved along with contextual information in compressed tar files stored under <i>/var/tmp/process-name.core.core-number.tgz</i> for debugging purposes.
Usage Guidelines	See “Core Dump Files” on page 284
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ntp

Syntax	<pre> ntp { authentication-key <i>number</i> <i>type</i> <i>type</i> <i>value</i> <i>password</i>; boot-server <i>address</i>; broadcast <<i>address</i>> <<i>key</i> <i>key-number</i>> <<i>version</i> <i>value</i>> <<i>ttl</i> <i>value</i>>; broadcast-client; multicast-client <<i>address</i>>; peer <i>address</i> <<i>key</i> <i>key-number</i>> <<i>version</i> <i>value</i>> <<i>prefer</i>>; server <i>address</i> <<i>key</i> <i>key-number</i>> <<i>version</i> <i>value</i>> <<i>prefer</i>>; trusted-key [<i>key-numbers</i>]; } </pre>
Hierarchy Level	[edit system]
Description	Configure the Network Time Protocol (NTP) on the router.
Options	The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Configure the Network Time Protocol” on page 266.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

peer

Syntax	<pre> peer <i>address</i> <<i>key</i> <i>key-number</i>> <<i>version</i> <i>value</i>> <<i>prefer</i>>; </pre>
Hierarchy Level	[edit system ntp]
Description	For NTP, configure the local router to operate in symmetric active mode with the remote system at the specified <i>address</i> . In this mode, the local router and the remote system can synchronize each other. This configuration is useful in a network in which either the local router or the remote system might be a better source of time.
Options	<p><i>address</i>—Address of the remote system. You must specify an address, not a hostname.</p> <p><i>key</i> <i>key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. Values: Any unsigned 32-bit integer</p> <p><i>prefer</i>—(Optional) Mark the remote system as the preferred host, which means that, if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p><i>version</i> <i>value</i>—(Optional) Specify the NTP version number to be used in outgoing NTP packets. Values: 1, 2, 3 Default: 3</p>
Usage Guidelines	See “Configure the NTP Time Server and Time Services” on page 267.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

permissions

Syntax	permissions [<i>permissions</i>];
Hierarchy Level	[edit system login class]
Description	Configure the login access privileges to be provided on the router.
Options	<i>permissions</i> —Privilege type. For a list of types, see Table 10, “Login Class Permission Bits” on page 255.
Usage Guidelines	See “Configure Access Privilege Levels” on page 254.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	user on page 318

port

Syntax	port <i>number</i> ;
Hierarchy Level	[edit system radius-server <i>address</i>]
Description	Configure the port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2138)
Usage Guidelines	See “Configure RADIUS Authentication” on page 241.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ports

Syntax	ports { auxiliary { type <i>terminal-type</i> ; } console { type <i>terminal-type</i> ; } }
Hierarchy Level	[edit system]
Description	Configure the properties of the console and auxiliary ports, which are located on the router’s craft interface.
Options	The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Configure Console and Auxiliary Port Properties” on page 277.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

processes

Syntax processes {
 inet-process (enable | disable) failover (alternate-media | other-routing-engine);
 interface-control (enable | disable) failover (alternate-media | other-routing-engine);
 mib-process (enable | disable) failover (alternate-media | other-routing-engine);
 ntp (enable | disable) failover (alternate-media | other-routing-engine);
 routing (enable | disable) failover (alternate-media | other-routing-engine);
 snmp (enable | disable) failover (alternate-media | other-routing-engine);
 watchdog (enable | disable) failover (alternate-media | other-routing-engine)
 timeout *seconds*;
 }

Hierarchy Level [edit system]

Description Configure which JUNOS software processes are running on the router.

Default All processes are enabled by default



Caution

Never disable any of the software processes unless instructed to do so by a customer support engineer.

Options failover (alternate-media | other-routing-engine)—(Optional) For routers with redundant Routing Engines only, switch to backup media if a process fails repeatedly. If a process fails three times in quick succession, the router reboots from the alternate media or the other Routing Engine.

timeout *seconds*—(Optional) How often the system checks the watchdog timer, in seconds. If the watchdog timer has not been checked in the specified number of seconds, the system reloads. If you set the time value too low, it is possible for the system to reboot immediately after it loads.

Values: 15, 60, 180

Default: 180 seconds (rounded up to 291 seconds by the JUNOS kernel)

Usage Guidelines See “Disable JUNOS Software Processes” on page 283.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

protocol-version

Syntax	protocol-version;
Hierarchy Level	[edit system services ssh]
Description	Specify secure shell (ssh) protocol version.
Options	protocol version—v1, v2, or [v1 v2] Default: [v2]
Usage Guidelines	See “Configure ssh Protocol Version” on page 282.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

radius-server

Syntax	radius-server <i>server-address</i> { port <i>number</i> ; retry <i>number</i> ; secret <i>password</i> ; timeout <i>seconds</i> ; }
Hierarchy Level	[edit system]
Description	Configure the Remote Authentication Dial-In User Service (RADIUS). To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
Options	<i>server-address</i> —Address of the RADIUS authentication server. The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Configure RADIUS Authentication” on page 241.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

retry

Syntax	<code>retry <i>number</i>;</code>
Hierarchy Level	[edit system radius-server <i>server-address</i>]
Description	Number of times that the router attempts to contact a RADIUS authentication server.
Options	<i>number</i> —Number of times to retry contacting a RADIUS server. Range: 1 through 10 Default: 3
Usage Guidelines	See “Configure RADIUS Authentication” on page 241.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
See Also	timeout on page 314

root-authentication

Syntax	<code>root-authentication { (encrypted-password "<i>password</i>" plain-text-password); ssh-rsa "<i>public-key</i>"; ssh-dsa "<i>public-key</i>"; }</code>
Hierarchy Level	[edit system]
Description	Configure the authentication methods for the root-level user, whose username is “root.”
Options	encrypted-password " <i>password</i> "—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password. plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password. ssh-rsa " <i>public-key</i> "—secure shell (ssh 1) authentication. Specify the ssh public key. You can specify one or more public keys. ssh-rsa " <i>public-key</i> "—secure shell (ssh 2) authentication. Specify the ssh public key. You can specify one or more public keys.
Usage Guidelines	See “Configure the Root Password” on page 239.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	authentication on page 286

root-login

Syntax	root-login (allow deny deny-password);
Hierarchy Level	[edit system services ssh]
Description	Control user access through ssh.
Options	allow—Allows users to log on to the router as root through ssh. Default: allow deny—Disable users from logging on the router as root through ssh. deny-password—Allows users to log onto the router as root through ssh when the authentication method (for example, RSA authentication) does not require a password.
Usage Guidelines	See “Configure Root Login” on page 282.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	“Configure ssh Service” on page 281.

secret

Syntax	secret <i>password</i> ;
Hierarchy Level	[edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>]
Description	Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router must match that used by the server.
Options	<i>password</i> —Password to use. Can include spaces.
Usage Guidelines	See “Configure RADIUS Authentication” on page 241 and “Configure TACACS+ Authentication” on page 243.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

server

Syntax	server <i>address</i> <key <i>key-number</i> > <version <i>value</i> > <prefer>;
Hierarchy Level	[edit system ntp]
Description	For NTP, configure the local router to operate in client mode with the remote system at the specified <i>address</i> . In this mode, the local router can be synchronized to the remote system, but the remote system never can be synchronized to the local router.
Options	<p><i>address</i>—Address of the remote system. You must specify an address, not a hostname.</p> <p>key <i>key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. Values: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as preferred host, which means that, if all other are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version <i>value</i>—(Optional) Specify the version number to be used in outgoing NTP packets. Values: 1, 2, 3 Default: 3</p>
Usage Guidelines	See “Configure the NTP Time Server and Time Services” on page 267.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

services

Syntax

```

services {
    finger {
        <connection-limit limit>;
        <rate-limit limit>;
    }

    rlogin {
        <connection-limit limit>;
        <rate-limit limit>;
    }

    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        <connection-limit limit>;
        <rate-limit limit >;
    }

    telnet {
        <connection-limit limit>;
        <rate-limit limit>;
    }
}

```

Hierarchy Level [edit system]

Description Configure the router so that users on remote systems can access the local router through the finger, rlogin, ssh, and telnet, and network utilities.

Options connection-limit *limit*—(Optional) Maximum number of established connections.
Range: 1 through 250
Default: 75

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.
Range: 1 through 250
Default: 150

finger—Allow finger requests from remote systems to the local router.

ftp—Allow ftp requests from remote systems to the local router.

rlogin—Allow rlogin access from remote systems to the local router.

ssh—Allow ssh access from remote systems to the local router.

telnet—Allow telnet login from remote systems to the local router.

The remaining statements are explained separately.

Usage Guidelines See “Configure System Services” on page 280.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

See Also protocol-version on page 306, root-login on page 308, and “Configure ssh Service” on page 281.

single-connection

Syntax	single-connection;
Hierarchy Level	[edit system tacplus-server server-address]
Description	Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt.
Usage Guidelines	See “Configure TACACS+ Authentication” on page 243.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

static-host-mapping

Syntax	static-host-mapping { <i>host-name</i> { inet [<i>address</i>]; sysid <i>system-identifier</i> ; alias [<i>alias</i>]; } }
Hierarchy Level	[edit system]
Description	Map a host name to one or more IP addresses and aliases, and configure an ISO system identifier (sysid).
Options	alias <i>alias</i> —(Optional) Alias for the host name. <i>host-name</i> —Fully qualified host name. inet <i>address</i> —IP address. You can specify one or more IP addresses for the host. sysid <i>system-identifier</i> —ISO system identifier (sysid). This is the 6-byte sysid portion of the IS-IS Network Service Access Point (NSAP). We recommend that you use the host's IP address represented in binary-coded decimal (BCD) format. For example, the IP address 208.197.169.18 would be 2081.9716.9018 in BCD.
Usage Guidelines	See “Configure the Router's Name and Addresses” on page 233.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

syslog

```

Syntax  syslog {
            file filename {
                facility level;
                archive {
                    files number;
                    size size;
                    (world-readable | no-world-readable);
                }
            }
            host hostname {
                facility level;
                facility-override facility;
                log-prefix string;
            }
            user (username | *) {
                facility level;
            }
            console {
                facility level;
            }
            archive {
                files number;
                size size;
                (world-readable | no-world-readable);
            }
        }

```

Hierarchy Level [edit system]

Description Configure the types of syslog messages to log to files, remote host, user terminals, and the system console.

Options archive—Configure how to archive system logging files.

console—Configure the types of syslog messages to log to the system console.

facility level—Class of log messages. To specify multiple classes, include multiple *facility level* options. These can include one or more of the facilities listed in Table 14, “System Logging Facilities” on page 272.

facility-override *facility*—When sending files to a remote host, override the facility.

file *filename*—Configure the types of syslog messages to log to the specified file. To log messages to more than one file, include more than one file option.

files *number*—Maximum number of system log files. When a log file named *syslog-file* reaches its maximum size, it is renamed as *syslog-file.0*, then as *syslog-file.1*, and so on, until the maximum number of log files is reached. Then, the oldest log file is overwritten.

Range: 1 through 1000

Default: 10 files

host *hostname*—Configure the types of syslog messages to log to the specified remote host. Specify the IP address or the fully qualified domain name of the host. To log messages to more than one host, include more than one host option.

	<i>level</i> —Priority of the message. This can be one or more of the priorities listed in Table 15.
	<i>log-prefix string</i> —When sending log messages to a remote host, prepend a string to the log message.
	<i>no-world-readable</i> —System logging files can be read only by a limited group of users. This is the default.
	<i>size size</i> —Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a system log file named <i>syslog-file</i> reaches this size, it is renamed as <i>syslog-file.0</i> . When the <i>syslog-file</i> again reaches its maximum size, <i>syslog-file.0</i> is renamed as <i>syslog-file.1</i> and <i>syslog-file</i> is renamed as <i>syslog-file.0</i> . This renaming scheme continues until the maximum number of log files is reached. Then, the oldest log file is overwritten. Syntax: <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB Range: 64 KB through 1 GB
	<i>user (username *)</i> —Configure the types of syslog messages to log to the specified user's terminal session. To log messages to more than one user, include more than one user option. To log messages to the terminal sessions of all users who are currently logged in, specify an asterisk instead of a <i>username</i> .
	<i>world-readable</i> —System logging files can be read by anyone. Default: <i>no-world-readable</i>
Usage Guidelines	See “Configure System Logging” on page 271.
Required Privilege Level	<i>system</i> —To view this statement in the configuration. <i>system-control</i> —To add this statement to the configuration.
See Also	The options statement in the <i>JUNOS Internet Software Configuration Guide: Routing and Routing Protocols</i> .

system

Syntax	<code>system { ... }</code>
Hierarchy Level	[edit]
Description	Configure system management properties.
Usage Guidelines	See “System Management Configuration Statements” on page 229.
Required Privilege Level	<i>system</i> —To view this statement in the configuration. <i>system-control</i> —To add this statement to the configuration.

tacplus-server

Syntax tacplus-server *server-address* {
 secret *password*;
 single-connection;
 timeout *seconds*;
 }

Description Configure the Terminal Access Controller Access Control System Plus (TACACS+).

Hierarchy Level [edit system]

Options *server-address*—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

Usage Guidelines See “Configure TACACS+ Authentication” on page 243.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

timeout

Syntax timeout *seconds*;

Hierarchy Level [edit system radius-server *server-address*],
 [edit system tacplus-server *server-address*]

Description Configure the amount of time that the local router waits to receive a response from a RADIUS or TACACS+ server.

Options *seconds*—Amount of time to wait.
 Range: 1 through 90
 Default: 3 seconds

Usage Guidelines See “Configure RADIUS Authentication” on page 241 and “Configure TACACS+ Authentication” on page 243.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

See Also retry on page 307

time-zone

Syntax	time-zone <i>time-zone</i> ;
Hierarchy Level	[edit system]
Description	Set the local time zone.
Default	UTC
Options	<p><i>time-zone</i>—Time zone. To have the time zone change take effect for all processes running on the router, you must reboot the router. Specify the time zone either as UTC, which is the default time zone, or use one of the following continent/country/zone primary names:</p> <p>Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek</p> <p>America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/El_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Regina, America/Rosario, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Tortola, America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife</p> <p>Antarctica/Casey, Antarctica/DumontD'Urville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/South_Pole</p> <p>Arctic/Longyearbyen</p> <p>Asia/Aden, Asia/Alma-Ata, Asia/Amman, Asia/Anadyr, Asia/Aqtou, Asia/Aqtobe, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hong_Kong, Asia/Irkutsk, Asia/Ishigaki, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk,</p>

Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Magadan, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Phnom_Penh, Asia/Pyongyang, Asia/Qatar, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimbu, Asia/Tokyo, Asia/Ujung_Pandang, Asia/Ulan_Bator, Asia/Urumqi, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan

Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley

Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Darwin, Australia/Hobart, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/Perth, Australia/Sydney

Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Helsinki, Europe/Istanbul, Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Oslo, Europe/Paris, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Warsaw, Europe/Zagreb, Europe/Zurich

Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion

Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap

Usage Guidelines See “Set the Time Zone” on page 265.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

trusted-key

Syntax	trusted-key [<i>key-numbers</i>];
Hierarchy Level	[edit system ntp]
Description	For NTP, configure the keys you are allowed to use when you configure the local router to synchronize its time with other systems on the network.
Options	<i>key-numbers</i> —One or more key numbers. Each key can be any 32-bit unsigned integer except 0.
Usage Guidelines	See “Configure NTP Authentication Keys” on page 269.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
See Also	authentication-key on page 287, broadcast on page 289, peer on page 303, server on page 309

uid

Syntax	uid <i>uid-value</i> ;
Hierarchy Level	[edit system login user]
Description	Configure user identifier for a login account.
Options	<i>uid-value</i> —Number associated with the login account. This value must be unique on the router. Range: 100 through 64,000
Usage Guidelines	See “Configure User Access” on page 253.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

user

Syntax user *user-name* {
 full-name *complete-name*;
 uid *uid-value*;
 class *class-name*;
 authentication {
 (encrypted-password "*password*" | plain-text-password);
 ssh-rsa "*public-key*";
 ssh-dsa "*public-key*";
 }
}

Hierarchy Level [edit login]

Description Configure access permission for individual users.

Options The remaining statements are explained separately in this chapter.

Usage Guidelines See "Configure User Access" on page 253.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

See Also class on page 290

Part 5

Access

- Access Configuration Guidelines on page 321



Chapter 26

Access Configuration Guidelines

To configure access, include statements at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
  authentication-order [ authentication-methods ];
  client name chap-secret data;
}
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
```

This chapter discusses the following topics:

- Configure Challenge Handshake Authentication Protocol on page 322
- Configure the Authentication Order on page 323
- Trace Access Processes on page 324
- Summary of Access Configuration Statements on page 325

Configure Challenge Handshake Authentication Protocol

The Challenge Handshake Authentication Protocol (CHAP) allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the local-name option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about local-name option, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

To configure CHAP, include the profile statement and specify a profile name at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
  client name chap-secret data;
}
```

Then reference the CHAP profile name at the [edit interfaces] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

You can configure multiple profiles. You can also configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret secret is the secret associated with that peer.

Example: PPP Challenge Handshake Authentication Protocol

Configure the profile pe-A-ppp-clients at the [edit access] hierarchy level, then reference it at the [edit interfaces] hierarchy level.

```
[edit]
access {
  profile pe-A-ppp-clients {
    client cpe-1 chap-secret "$1$dQYsZ$B5qjUeUjDsUo.yKwcCZ0"; # SECRET-DATA
    client cpe-2 chap-secret "$1$kdAsfaDAfkDjDsASxfafKdFKJ";   # SECRET-DATA
  }
}
```

```

interfaces {
  so-1/1/1 {
    encapsulation ppp;
    ppp-options {
      chap {
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/1";
      }
    }
  }
  so-1/1/2 {
    encapsulation ppp;
    ppp-options {
      chap {
        passive;
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/2";
      }
    }
  }
}

```

Configure the Authentication Order

You can configure the order in which the JUNOS software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure the authentication order, include the `authentication-order` statement at the [edit access profile *profile-name*] hierarchy level:

```

[edit access profile profile-name]
authentication-order [ authentication-methods ];

```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

- **radius**—Verify the client using RADIUS authentication services.
- **password**—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

If you do not include the `authentication-order` statement, clients are verified by means of password authentication.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer than that to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers such that the number of times the router attempts to contact each server is three times, and that with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 29 seconds. If you add more RADIUS servers to this configuration, they may not be contacted because the authentication process may be abandoned before these servers are tried.

The JUNOS software enforces a limit to the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—may fail to authenticate a client when this limit is exceeded. In the above example, any authentication method following this method is tried. If it fails, the authentication sequence is reinitiated by the router until authentication succeeds and the link is brought up.

RADIUS authentication servers are configured at the [edit system radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see “Configure RADIUS Authentication” on page 241.

Trace Access Processes

To trace access processes, you can specify options in the traceoptions statement at the [edit access] hierarchy level:

```
[edit access]
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
```

You can specify the following access tracing flags:

- all—All tracing operations
- authentication—All authentication module-handling
- chap—All CHAP messages and handling
- configuration—Reading of configuration
- radius—All RADIUS messages and handling

Summary of Access Configuration Statements

The following sections explain each of the access configuration statements. The statements are organized alphabetically.

authentication-order

Syntax	authentication-order [authentication-methods];
Hierarchy Level	[edit access profile <i>profile-name</i>]
Description	Sets the order in which the JUNOS software tries different authentication methods when verifying that a client can access the router. For each login attempt, the software tries the authentication methods in order, from first to last.
Usage Guidelines	See “Configure the Authentication Order” on page 323.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

profile

Syntax	profile <i>profile-name</i> { client <i>name</i> chap-secret <i>data</i> ; }
Hierarchy Level	[edit access]
Description	Configure PPP CHAP.
Options	profile <i>name</i> —Mapping between peer identifiers and CHAP secret keys. This is the entity that is queried for the secret key whenever a CHAP challenge or response is received. client <i>name</i> —Peer identity. chap-secret <i>data</i> —CHAP secret associated with the given peer identity.
Usage Guidelines	See “Configure Challenge Handshake Authentication Protocol” on page 322.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

traceoptions

Syntax traceoptions {
 flag all;
 flag authentication;
 flag chap;
 flag configuration;
 radius;
 }

Hierarchy Level [edit access]

Description Configure access tracing options.

To specify more than one tracing operation, include multiple flag statements.

Options flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

Access Tracing Flags

- all—All tracing operations
- authentication—All authentication module-handling
- chap—All CHAP messages and handling
- configuration—Reading of configuration
- radius—All RADIUS messages and handling

Usage Guidelines See “Trace Access Processes” on page 324.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Part 6

Security Services

- Security Services Overview on page 329
- Security Services Configuration Guidelines on page 333
- Summary of Security Services Configuration Statements on page 361

Chapter 27

Security Services Overview

The JUNOS software supports IPSec. This chapter discusses the following topics, which provide background information related to configuring IPSec:

- IPSec Overview on page 329
- Security Associations on page 330
- IPSec Security on page 330
- IKE on page 331

For a list of IPSec- and IKE-supported standards, see “IPSec and IKE” on page 23.

IPSec Overview

The Internet Protocol Security (IPSec) architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

IPSec also defines a security association and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. IPSec provides secure tunnels between two peers.

Security Associations

To use IPSec security services, you create SAs between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPSec. There are two types of SAs: manual and dynamic.

- Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the Security Parameter Index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic SAs require additional configuration. With dynamic SAs, you configure IKE first and then the SA. IKE creates dynamic security associations; it negotiates SAs for IPSec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPSec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPSec SAs.

IPSec Security

The JUNOS software implementation of IPSec supports two types of security—host-to-host and gateway-to-gateway:

- Host-to-Host Protection on page 330
- Gateway-to-Gateway Protection on page 330

Host-to-Host Protection

Host-to-host security protects BGP sessions with other routers. Any SA to be used with BGP must be configured manually, and must use transport mode. Static values must be configured on both ends of the security association.

To apply host protection, configure manual SAs in transport mode and then reference the SA by name at the [edit protocols bgp] hierarchy level to protect a session with a given peer. For more information about how to reference the configured SA, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

Gateway-to-Gateway Protection

Gateway-to-gateway security protects traffic traveling between two security gateways. It is most often used to encrypt virtual private network (VPN) traffic. Because of the high speeds of the transit interfaces, this functionality requires an ES PIC.

To enable gateway-to-gateway protection, complete the following steps:

1. Configure IKE (for dynamic SAs only)
2. Configure an SA
3. Configure an ES PIC
4. Configure traffic parameters

IKE

IKE is a key management protocol that creates dynamic SAs; it negotiates SAs for IPSec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE does the following:

- Negotiates and manages IKE and IPSec parameters
- Authenticates secure key exchange
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys
- Provides identity protection (in main mode)

IKE occurs over two phases. In the first phase, it negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In the second phase, inbound and outbound IPSec SAs are established. The IKE SA secures the exchanges in the second phase. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.

.....

Chapter 28

Security Services Configuration Guidelines

To configure security services, include statements at the [edit security] hierarchy level:

```
[edit security]
certificates local certificate-name;
ike {
    numerous global IKE statements
    proposal ike-proposal-name {
        authentication-algorithm (md5 | sha1);
        authentication-method pre-shared-keys;
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
    }
    policy ike-peer-address {
        mode (aggressive | main);
        proposal [ike-proposal-names];
        pre-shared-key (ascii-text key | hexadecimal key);
    }
}
ipsec {
    numerous global ipsec statements
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol esp;
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposal [ipsec-proposal-names];
    }
}
security-association name {
    mode (tunnel | transport);
```

```

manual {
  direction (inbound | outbound | bi-directional) {
    spi spi-value;
    protocol (esp | ah);
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
  }
}

dynamic {
  <replay-window-size (32 | 64)>;
  ipsec-policy policy-name;
}

traceoptions {
  file <files number> < size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}

```



Note

Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

This chapter describes the following tasks for configuring Internet Protocol Security (IPSec) and the Internet Key Exchange (IKE):

- Minimum IPSec Configuration on page 335
- Configure Global IPSec Properties on page 336
- Configure IPSec Proposal Properties on page 336
- Configure Security Associations on page 337
- Host-to-Host Security on page 338
- Configure IKE (Dynamic SAs Only) on page 344
- Configure an IKE Policy on page 347
- Configure an IPSec Proposal on page 350
- Configure an IPSec Policy on page 352
- Configure Traceoptions on page 354

- Configure the ES PIC on page 354
- Configure Traffic on page 355
- Configure an ES Tunnel Interface for a Layer 3 VPN on page 360

Minimum IPSec Configuration

This section includes the following minimum configurations:

- Minimum Manual SA Configuration on page 335
- Minimum Dynamic SA Configuration on page 335

Minimum Manual SA Configuration

```
[edit security ipsec]
security-association name {
  manual {
    direction (inbound | outbound | bi-directional) {
      spi spi-value;
      protocol (esp | ah);
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
    }
  }
}
```

Minimum Dynamic SA Configuration

```
[edit security]
ike {
  proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method pre-shared-keys;
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc);
  }
  policy ike-peer-address {
    proposal [ike-proposal-names];
    pre-shared-key (ascii-text key | hexadecimal key);
  }
}
```

```

ipsec {
  policy ipsec-policy-name {
    proposal [ipsec-proposal-names];
  }
  proposal ipsec-proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    encryption-algorithm (3des-cbc | des-cbc);
    protocol esp;
  }
  security-association name {
    dynamic {
      ipsec-policy policy-name;
    }
  }
}

```

Configure Global IPSec Properties

To configure IPSec, you include statements at the [edit security ipsec] hierarchy level. Many of the global IPSec- and proposal-specific statements are identical. When you can configure the same statement at more than one level, the more-specific statement overrides the less-specific statement. For example, a proposal-specific statement overrides a global IPSec statement.

To define global IPSec properties, which apply to all IPSec proposals, include one or more of the following statements at the [edit security ipsec] hierarchy level. These statements are explained separately.

```

[edit security ipsec]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
encryption-algorithm (3des-cbc | des-cbc);
lifetime-seconds seconds;
protocol esp;

```

Configure IPSec Proposal Properties

To define IPSec proposal-specific properties, include one or more of the following statements at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level. The statements are explained separately.

```

[edit security ipsec proposal ipsec-proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
encryption-algorithm (3des-cbc | des-cbc);
lifetime-seconds seconds;
protocol esp;

```

For more information about how to configure an IPSec proposal, see “Configure an IPSec Proposal” on page 350.

Configure Security Associations

To use IPSec security services, you create a security association (SA) between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPSec. You can configure two types of SAs:

- **Manual**—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see “Configure Manual Security Associations” on page 339.
- **Dynamic**—Specifies proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposal statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see “Configure the ES PIC” on page 354.



Note

The JUNOS software does not perform a commit check when an SA name referenced in the BGP protocol section is not configured at the [edit security ipsec] hierarchy level.

We recommend that you configure no more than 512 dynamic security associations per ES PIC.

To configure an SA for IPSec, include the security-association statement and specify a security association name at the [edit security ipsec] hierarchy level:

```
[edit security ipsec]
security-association name;
```

This section describes the following topics related to configuring security associations:

- Host-to-Host Security on page 338
- Configure IPSec Mode on page 338
- Configure Manual Security Associations on page 339
- Configure Dynamic Security Associations on page 343

IPSec Security

The JUNOS software implementation of IPSec supports two types of security: host-to-host and gateway-to-gateway.



Note

The JUNOS software does not support IPv6 or digital certificates for IPSec.

Host-to-Host Security

Host-to-host security protects BGP sessions with other routers. Any SA to be used with BGP must be configured manually and use transport mode. Static values must be configured on both ends of the security association.

To configure IPsec security, include the mode statement and specify transport at the [edit security ipsec security-association *name*] hierarchy level:

```
[edit security ipsec security-association name]  
mode (tunnel | transport);
```

To apply host protection, you configure manual SAs in transport mode and then reference the SA by name at the [edit protocols bgp] hierarchy level to protect a session with a given peer. For more information about how to reference the configured SA, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

Gateway-to-Gateway Security

Gateway-to-gateway security protects traffic traveling between two security gateways. It is most often used to encrypt virtual private network (VPN) traffic. Because of the high speeds of the transit interfaces, this functionality requires an ES PIC. For more information on about how to configure gateway-to-gateway protection, see “Configure IPsec Mode” on page 338.

Configure IPsec Mode

IPsec runs in two modes: transport and tunnel. By default, tunnel mode is enabled. Tunnel mode protects connections between security gateways. For information about when to use transport mode, see “Host-to-Host Security” on page 338.

To configure the IPsec in tunnel mode, include the mode statement and specify tunnel at the [edit security ipsec security-association *name*] hierarchy level:

```
[edit security ipsec security-association name]  
mode (tunnel | transport);
```



Note

Tunnel mode requires the ES PIC.

The JUNOS software supports only ESP when you use tunnel mode.

In transport mode, the JUNOS software does not support AH and encapsulating security payload (ESP) header bundles.

To enable gateway-to-gateway protection, follow these steps:

1. Configure IKE (Dynamic SAs Only) on page 344
2. Configure Security Associations on page 337
3. Configure the ES PIC on page 354
4. Configure Traffic on page 355

For more information about the ES PIC, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Configure Manual Security Associations

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place.

To configure the manual IPSec security association, include statements at the [edit security ipsec security-association *name* manual] hierarchy level:

```
[edit security ipsec security-association name manual]
direction (inbound | outbound | bi-directional) {
  spi spi-value;
  protocol (esp | ah);
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  encryption {
    algorithm (des-cbc | 3des-cbc);
    key (ascii-text key | hexadecimal key);
  }
}
```

To configure manual SA statements, do the following:

- Configure Direction on page 340
- Configure the Protocol on page 341
- Configure a Security Parameter Index (SPI) on page 341
- Configure Authentication on page 341
- Configure Encryption on page 342

Configure Direction

The direction statement sets inbound and outbound IPSec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the inbound and outbound options. If you want the same attributes in both directions, use the bidirectional option.

To configure the direction of IPSec processing, include the direction statement and specify the direction at the [edit security ipsec security-association *name* manual] hierarchy level:

```
[edit security ipsec security-association name manual]
direction (inbound | outbound | bidirectional);
```

Example: Configure Inbound and Outbound Direction statements

Define different algorithms, keys, and security parameter index values for each direction.

```
[edit security ipsec security-association name
manual {
  direction inbound {
    protocol esp;
    spi 16384;
    encryption {
      algorithm 3des-cbc;
      key ascii-text 23456789012345678901234;
    }
  }
  direction outbound {
    protocol esp;
    spi 24576;
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
  }
}
```

Example: Configure Bidirectional Statement

Define the same algorithms, keys, and security parameter index values for each direction.

```
[edit security ipsec security-association name manual]
direction bidirectional {
  protocol ah;
  spi 20001;
  authentication {
    algorithm hmac-md5-96;
    key ascii-text 123456789012abcd;
  }
}
```


Configure the Protocol

IPSec uses two protocols to protect IP traffic: ESP and AH. For transport mode SAs, both ESP and AH are supported.

To configure the IPSec protocol, include the protocol statement and specify esp or ah at the [edit security ipsec security-association *name* manual direction (inbound | outbound | bidirectional) hierarchy level:

```
[edit security ipsec security-association name manual direction (inbound | outbound |
bi-directional)]
protocol (esp | ah);
```

Configure a Security Parameter Index (SPI)

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.



Each manual SA must have a unique SPI and protocol combination.

To configure the SPI, include the spi statement and specify a value (256 through 16,639) at the [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional) hierarchy level:

```
[edit security ipsec security-association name manual direction (inbound | outbound |
bi-directional)]
spi spi-value;
```

Configure Authentication

To configure an authentication algorithm, include the authentication statement and specify an authentication algorithm and a key at the [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional)] hierarchy level:

```
[edit security ipsec security-association name manual direction (inbound | outbound |
bidirectional)]
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- hmac-md5-96—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- hmac-sha1-96—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the `hmac-md5-96` option, the key contains 16 ASCII characters. With the `hmac-sha1-96` option, the key contains 20 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the `hmac-md5-96` option, the key contains 32 hexadecimal characters. With the `hmac-sha1-96` option, the key contains 40 hexadecimal characters.

Configure Encryption

To configure IPSec encryption, include the encryption statement and specify an algorithm and key at the [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional)] hierarchy level:

```
[edit security ipsec security-association name manual direction (inbound | outbound |
bi-directional)]
encryption {
  algorithm (des-cbc | 3des-cbc);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.



Note

For a list of DES Weak and Semi-Weak keys, see RFC 2409.

For 3des-cbc, the first 8 bytes must not be same as the second 8 bytes, and the second 8 bytes must not be same as the third 8 bytes.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the `des-cbc` option, the key contains 8 ASCII characters. With the `3des-cbc` option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the `des-cbc` option, the key contains 16 hexadecimal characters. With the `3des-cbc` option, the key contains 48 hexadecimal characters.



Note

You cannot configure encryption when you use authentication header protocol (AH).

Configure Dynamic Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To enable a dynamic SA, follow these steps:

1. Configure IKE proposals and IKE policies associated with these proposals.
2. Configure IPsec proposals and an IPsec policy associated with these proposals.
3. Associate an SA with an IPsec policy.

For more information about IKE policies and proposals, see “Configure IKE (Dynamic SAs Only)” on page 344. For more information about IPsec policies and proposals, see “Configure an IPsec Policy” on page 352.



Note

The JUNOS software supports only the ESP protocol when you use tunnel mode SAs. Dynamic tunnel SAs require an ES PIC.

The JUNOS software supports only manual SAs in transport mode; static values must be configured on both routers.

To configure a dynamic SA, include the `dynamic` statement and specify a 32- or 64-packet replay window size and an IPsec policy name at the `[edit security ipsec security-association name]` hierarchy level. The `window-replay-size` statement is optional.

```
[edit security ipsec security-association name]
dynamic {
  replay-window-size (32 | 64);
  ipsec-policy policy-name;
}
```



Note

If you want to establish a dynamic SA, the attributes in at least one configured IPsec and IKE proposal must match those of its peer.

The replay window is not used with manual SAs.

Configure IKE (Dynamic SAs Only)

Dynamic SAs require Internet Key Exchange (IKE) configuration. With dynamic SAs, you configure IKE first, and then the SA. IKE creates dynamic SAs; it negotiates SAs for IPSec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway.

This section describes the following IKE topics:

- IKE Global Properties on page 344
- IKE Proposal Properties on page 344
- Configure an IKE Proposal on page 345

IKE Global Properties

To configure IKE, include statements at the [edit security ike] hierarchy level. Many of the global IKE- and proposal-specific statements are identical. When you configure the same statement at more than one level in the hierarchy, the more-specific statement overrides the less-specific statement. For example, a proposal-specific statement overrides a global IKE statement.

To define global IKE properties, which apply to all IKE proposals, include one or more of the following statements at the [edit security ike] hierarchy level. These statements are explained separately.

```
[edit security ike]
authentication-algorithm (md5 | sha1);
authentication-method pre-shared-keys;
dh-group (group1 | group2);
encryption-algorithm (3des-cbc | des-cbc);
lifetime-seconds seconds;
```

IKE Proposal Properties

To define proposal-specific properties, include one or more of the following statements at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name]
authentication-algorithm (md5 | sha1);
authentication-method pre-shared-keys;
dh-group (group1 | group2);
encryption-algorithm (3des-cbc | des-cbc);
lifetime-seconds seconds;
```



Note

The JUNOS software supports only preshared keys for IKE.

Configure an IKE Proposal

You can configure one or more IKE proposals. Each proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer.

To configure an IKE proposal, include the proposal statement and specify a name at the [edit security ike] hierarchy level:

```
[edit security ike]
proposal ike-proposal-name;
```

This section discusses the following topics related to configuring an IKE proposal:

- Configure an IKE Authentication Algorithm on page 345
- Configure an IKE Authentication Method on page 345
- Configure an IKE Diffie-Hellman Group on page 346
- Configure an IKE Encryption Algorithm on page 346
- Configure IKE Lifetime on page 346
- Example: IKE Proposal Configuration on page 347

Configure an IKE Authentication Algorithm

To configure an IKE authentication algorithm, include the authentication-algorithm statement:

```
authentication-algorithm (md5 | sha1);
```

The authentication algorithm can be one of the following:

- md5—Produces a 128-bit digest.
- sha1—Produces a 160-bit digest.

To configure the IKE authentication algorithm globally for all IKE proposals, include this statement at the [edit security ike] hierarchy level. To configure an individual IKE proposal, include this statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level.

Configure an IKE Authentication Method

To configure an IKE authentication method, include the authentication-method statement and specify pre-shared-keys.

```
authentication-method pre-shared-keys;
```

To configure the IKE authentication method globally for all IKE proposals, include this statement at the [edit security ike] hierarchy level. To configure an individual IKE proposal, include this statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level.

Configure an IKE Diffie-Hellman Group

Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.

To configure an IKE Diffie-Hellman group, include the `dh-group` statement:

```
dh-group (group1 | group2);
```

The group can be one of the following:

- `group1`—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- `group2`—Specifies that IKE use the 1,024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

`group2` provides more security but requires more processing time.

To configure the Diffie-Hellman group globally for all IKE proposals, include this statement at the `[edit security ike]` hierarchy level. To configure an individual IKE proposal, include this statement at the `[edit security ike proposal ike-proposal-name]` hierarchy level.

Configure an IKE Encryption Algorithm

To configure an IKE encryption algorithm, include the `encryption-algorithm` statement:

```
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- `3des-cbc`—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- `des-cbc`—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.

To configure the IKE encryption algorithm globally for all IKE proposals, include this statement at the `[edit security ike]` hierarchy level. To configure an individual IKE proposal, include the statement at the `[edit security ike proposal ike-proposal-name]` hierarchy level.

Configure IKE Lifetime

The IKE lifetime sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or terminated.

To configure IKE lifetime, include the `lifetime-seconds` statement and specify the number of seconds (180 through 86,400):

```
lifetime-seconds seconds;
```

To configure the IKE lifetime globally for all IKE proposals, include this statement at the `[edit security ike]` hierarchy level. To configure an individual IKE proposal, include this statement at the `[edit security ike proposal ike-proposal-name]` hierarchy level.

Example: IKE Proposal Configuration

Define an IKE proposal:

```
[edit security ike]
proposal ike-proposal {
  authentication-method pre-shared-keys;
  dh-group group1;
  authentication-algorithm sha1;
  encryption-algorithm 3des-cbc;
}
```

Configure an IKE Policy

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address, the preshared key for the given peer, and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the policy statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the policy statement and specify a peer address at the [edit security ike] hierarchy level:

```
[edit security ike]
policy ike-peer-address [ike-proposal];
```



Note

The IKE policy peer address must be an IPSec tunnel destination address.

This section discusses the following topics related to configuring an IKE policy:

- Configure IKE Policy Mode on page 348
- Configure IKE Policy Proposal on page 348
- Configure IKE Policy Preshared Key on page 348

For an example of an IKE policy configuration, see “Example: Configure IKE Policy” on page 349.

Configure IKE Policy Mode

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.

To configure IKE policy mode, include the mode statement and specify aggressive or main at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]  
mode (aggressive | main);
```

Configure IKE Policy Proposal

The IKE policy proposal is a list of one or more proposals associated with an IKE policy.

To configure an IKE policy proposal, include the proposal statement and specify one or more proposal names at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]  
proposal [ike-proposal-names];
```

Configure IKE Policy Preshared Key

IKE policy preshared keys authenticate peers. You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

To configure an IKE policy preshared key, include the pre-shared-key statement and a key at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]  
pre-shared-key (ascii-text key | hexadecimal key);
```


Example: Configure IKE Policy

Define two IKE policies: policy 10.1.1.2 and policy 10.1.1.1. Each policy is associated with proposal-1 and proposal-2.

```
[edit security]
ike {
  proposal proposal-1 {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 1000;
  }
  proposal proposal-2 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 10000;
  }
  policy 10.1.1.2 {
    mode main;
    proposals [ proposal-1 proposal-2 ];
    pre-shared-key ascii-text example-pre-shared-key;
  }
  policy 10.1.1.1 {
    mode aggressive;
    proposals [ proposal-2 proposal-1 ];
    pre-shared-key hexadecimal 0102030abcbd;
  }
}
```

**Note**

Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see the *JUNOS Internet Software Operational Mode Command Reference*.

Configure an IPSec Proposal

An IPSec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPSec peer.

To configure an IPSec proposal, include the proposal statement and specify an IPSec proposal name at [edit security ipsec] hierarchy level:

```
[edit security ipsec]
proposal ipsec-proposal-name;
```

This section discusses the following topics related to configuring an IPSec proposal:

- Configure an Authentication Algorithm on page 350
- Configure an Encryption Algorithm on page 350
- Configure IPSec Lifetime on page 351
- Configure Protocol for Dynamic SA on page 351

Configure an Authentication Algorithm

To configure an IPSec authentication algorithm, include the authentication-algorithm statement:

```
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit digest.

To configure the authentication algorithm globally for all IPSec proposals, include this statement at the [edit security ipsec] hierarchy level. To configure an individual IPSec proposal, include this statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level.

Configure an Encryption Algorithm

To configure an IPSec encryption algorithm, include the encryption-algorithm statement:

```
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.

To configure the encryption algorithm globally for all IPSec proposals, include this statement at the [edit security ipsec] hierarchy level. To configure an individual IPSec proposal, include the statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:



Note

We recommend that you use the 3DES-CBC encryption algorithm.

Configure IPSec Lifetime

The IPSec lifetime option sets the lifetime of an IPSec SA. When the IPSec SA expires, it is replaced by a new SA (and SPI) or terminated. If you do not configure a lifetime and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.

To configure the IPSec lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400):

```
lifetime-seconds seconds;
```

To configure the lifetime globally for all IPSec proposals, include this statement at the [edit security ipsec] hierarchy level. To configure an individual IPSec proposal, include the statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level.



Note

When a dynamic SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPSec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires.

Configure Protocol for Dynamic SA

The protocol statement sets the protocol for a dynamic SA. The ESP protocol can support authentication, encryption, or both.



Note

The JUNOS software supports only ESP in tunnel mode.

To configure the protocol for a dynamic SA, include the protocol statement and specify the esp option:

```
protocol esp;
```

To configure the protocol globally for all IPSec proposals, include this statement at the [edit security ipsec] hierarchy level. To configure an individual IPSec proposal, include this statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level.

Configure an IPsec Policy

An IPsec policy defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPsec negotiation, IPsec looks for an IPsec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPsec proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IPsec proposals first; then you associate these proposals with an IPsec policy. You can then prioritize a list of proposals used by IPsec in the policy statement by listing the proposals you want to use, from first to last.

To configure an IPsec policy, include the policy statement, specify the policy name and one or more proposals you want to associate with this policy at the [edit security ipsec] hierarchy level:

```
[edit security ipsec]
policy ipsec-policy-name;
```

This section discusses the following topics related to configuring an IPsec policy:

- Configure Perfect Forward Secrecy on page 352
- Example: IPsec Policy Configuration on page 353

Configure Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the perfect-forward-secrecy statement and specify a Diffie-Hellman group at the [edit security ipsec policy *ipsec-policy-name*] hierarchy level.

```
perfect-forward-secrecy {
  keys (group1 | group2);
}
```

The key can be one of the following:

- group1—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- group2—Specifies that IKE use the 1,024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security than group1, but requires more processing time.

Example: IPSec Policy Configuration

Defines an IPSec policy, dynamic policy-1, that is associated with two proposals (dynamic-1 and dynamic-2):

```
[edit security ipsec]
proposal dynamic-1 {
  protocol esp;
  authentication-algorithm hmac-md5-96;
  encryption-algorithm 3des-cbc;
  lifetime-seconds 6000;
}
proposal dynamic-2 {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm 3des-cbc;
  lifetime-seconds 6000;
}
policy dynamic-policy-1 {
  perfect-forward-secrecy {
    keys group1;
  }
  proposals [ dynamic-1 dynamic-2 ];
}
security-association dynamic-sa1 {
  dynamic {
    replay-window-size 64;
    ipsec-policy dynamic-policy-1;
  }
}
```



Note

Updates to the current IPSec proposal and policy configuration are not applied to the current IPSec SA; updates are applied to new IPSec SAs.

If you want the new updates to take immediate effect, you must clear the existing IPSec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPSec security association, see *JUNOS Internet Software Operational Mode Command Reference*.

Configure Traceoptions

To configure security traceoptions, you can specify options in the traceoptions statement at the [edit security] hierarchy level:

```
[edit security]
traceoptions {
  file <files number> < size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}
```

The output of the security tracing options is placed in the /var/log/kmd.

You can specify one or more of the following security tracing flags:

- all—Trace all security events
- database—Trace database events
- general—Trace general events
- ike—Trace IKE module processing
- parse—Trace configuration processing
- policy-manager—Trace policy manager processing
- routing-socket—Trace routing socket messages
- timer—Trace internal timer events

Configure the ES PIC

Configuring the ES PIC associates the configured SA with a logical interface. This configuration defines the tunnel itself (logical subunit, tunnel addresses, maximum transmission unit [MTU], optional interface addresses, and the name of the SA to apply to traffic).

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.



Note

The tunnel source address must be configured locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The M5, M10, M20, and M40 routers support the ES PIC.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs. For more information about the ES PIC, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Example: ES PIC Configuration

Configures an IPsec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The ipsec-sa statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source tunnel 10.5.5.5;           # tunnel source address
      destination 10.6.6.6;           # tunnel destination address
    }
    family inet {
      ipsec-sa ipsec-sa;               # name of security association to apply to packet
      address 10.1.1.8/32 {            # local interface address inside local VPN
        destination 10.2.2.254;        # destination address inside remote VPN
      }
    }
  }
}
```

Configure Traffic

This section contains the following topics:

- Traffic Overview on page 356
- Example 1: Configure Outbound Traffic Filter on page 357
- Example 2: Apply Outbound Traffic Filter on page 358
- Example 3: Configure Inbound Traffic Filter for Policy Check on page 358
- Example 4: Apply Inbound Traffic Filter to ES PIC for Policy Check on page 359

Traffic Overview

Traffic configuration defines the traffic that must flow through the tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt off of that LAN or WAN. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure the configuration is correct. Make sure that you configure the router very carefully.

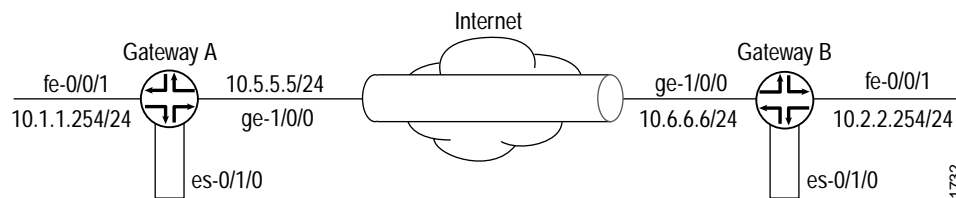


Note

The valid firewall filters statements for IPSec are destination-port, source-port, protocol, destination-address, and source-address.

In Figure 9, Gateway A protects the network 10.1.1.0/24, and Gateway B protects the network 10.2.2.0/24. The gateways are connected by an IPSec tunnel. For more information about firewalls, see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

Figure 9: Example: IPSec Tunnel Connecting Security Gateways



The SA and ES interface for security Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text 123456789009876543211234;
      }
    }
  }
}
```



```
[edit interfaces es-0/1/0]
unit 0 {
  tunnel {
    source 10.5.5.5;
    destination 10.6.6.6;
  }
  family inet {
    ipsec-sa manual-sa1;
    address 10.1.1.8/32 {
      destination 10.2.2.254;
    }
  }
}
```

Example 1: Configure Outbound Traffic Filter

Firewall filters for outbound traffic direct the traffic through the desired IPSec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see Figure 9). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal VPN traffic:

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address {      # local network
        10.1.1.0/24;
      }
      destination-address { # remote network
        10.2.2.0/24;
      }
    }
    then ipsec-sa manual-sa1; # apply SA name to packet
  }
  term default {
    then accept;
  }
}
```



The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

Example 2: Apply Outbound Traffic Filter

After you've configured the outbound firewall filter, you apply it:

```
[edit interfaces]
fe-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input ipsec-encrypt-policy-filter;
      }
      address 10.1.1.254/24;
    }
  }
}
```

The outbound filter is applied on the Fast Ethernet interface at the [edit interfaces fe-0/0/1 unit 0 family inet] hierarchy level. Any packet matching the IPSec action term (term 1) on the input filter (ipsec-encrypt-policy-filter), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the [edit interfaces es-0/1/0 unit 0 family inet] hierarchy level. So, if a packet arrives from the source address 10.1.1.0/24 and goes to the destination address 10.2.2.0/24, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the manual-sa1 SA. The ES PIC receives the packet, applies the manual-sa1 SA, and sends the packet through the tunnel.

The router must have a route to the tunnel endpoint; add a static route if necessary.

Example 3: Configure Inbound Traffic Filter for Policy Check

Here, an inbound firewall filter, which performs the final IPSec policy check, is created on security gateway A. This check ensures that only packets that match the traffic configured for this tunnel are accepted.

```
filter ipsec-decrypt-policy-filter {
  term term1 {
    from {
      source-address {
        10.2.2.0/24;
      }
      destination-address {
        10.1.1.0/24;
      }
    }
    then accept;
  }
}
```

Example 4: Apply Inbound Traffic Filter to ES PIC for Policy Check

After you create the inbound firewall filter, apply it to the ES PIC. Here, the inbound firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. The IPsec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and decrypts the incoming packet.

```
[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5;           # tunnel source address
      destination 10.6.6.6;     # tunnel destination address
    }
    family inet {
      filter {
        input ipsec-decrypt-policy-filter;
      }
      ipsec-sa manual-sa1;       # SA name applied to packet
      address 10.1.1.8/32 {      # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's security parameter index (SPI), protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPsec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and is used to decrypt the incoming packet. When the packets are processed (decrypted, authenticated, or both), the input firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. Term1 defines the decrypted (and verified) traffic and performs the required policy check.



Note

The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

Configure an ES Tunnel Interface for a Layer 3 VPN

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the PE router and on the CE router. You also need to configure Internet Protocol Security (IPSec) on the PE and CE routers. For more information about configuring an ES tunnel for a Layer 3 VPN, see the *JUNOS Internet Software Configuration Guide: VPNs*.

Configure JUNOScript XML-SSL Service

The Secure Sockets Layer (SSL) protocol uses public-private key technology, which requires a paired private key and authentication certificate xml-ssl service. This section describes how to import the SSL certificate into the JUNOScript server machine. For a complete example on how to configure the xml-ssl service, see the *JUNOScript API Guide*.



Note

Configuring xml-ssl service does not apply to IPSec.

To import an SSL certificate into the router, include the local statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
local certificate-name;
```

Enter CLI configuration mode on the JUNOScript server machine and issue the following commands at the [edit security certificates] and [edit security certificates local certificate-name] hierarchy levels to import the certificate.

```
[edit security certificates]
user@host# edit local certificate-name
```

where *certificate-name* is the name of the certificate.

```
[edit security certificates local certificate-name]
user@host# set load-key-file URL_or_path
```

where *URL_or_Path* is the URL or pathname on the local disk.



Note

The CLI expects the private key in the specified file (*URL_or_path*) to be unencrypted. If the key is encrypted, the CLI prompts for the passphrase associated with it, decrypts it, and stores the unencrypted version.

Chapter 29

Summary of Security Services Configuration Statements

The following sections explain each of the security services configuration statements. The statements are organized alphabetically.

authentication

Syntax	<pre>authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text key hexadecimal key); }</pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bi-directional)]
Description	Configure IPSec authentication parameters for manual SA.
Options	<p>algorithm—Hash algorithm that authenticates packet data.</p> <p>The algorithm can be one of the following:</p> <ul style="list-style-type: none">■ hmac-md5-96—Produces a 128-bit digest.■ hmac-sha1-96—Produces a 160-bit digest. <p>key—Type of authentication key.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none">■ ascii-text key—ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters.■ hexadecimal key—Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.
Usage Guidelines	See “Configure Authentication” on page 341.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm

authentication-algorithm (IKE)

Syntax	authentication-algorithm (md5 sha1);
Hierarchy Level	[edit security ike], [edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure IKE authentication algorithm.
Options	authentication-algorithm—Hash algorithm that authenticates packet data. md5—Produces a 128-bit digest. sha1—Produces a 160-bit digest.
Usage Guidelines	See “Configure an IKE Authentication Algorithm” on page 345.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm (IPSec)

Syntax	authentication-algorithm (hmac-md5-96 hmac-sha1-96);
Hierarchy Level	[edit security ipsec], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure IPSec authentication algorithm.
Options	authentication-algorithm—Hash algorithm that authenticates packet data. ■ hmac-md5-96—Produces a 128-bit digest. ■ hmac-sha1-96—Produces a 160-bit digest.
Usage Guidelines	See “Configure an Authentication Algorithm” on page 350.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-method

Syntax	authentication-method pre-shared-keys;
Hierarchy Level	[edit security ike], [edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure IKE authentication method.
Options	pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange.
Usage Guidelines	See “Configure an IKE Authentication Method” on page 345.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

certificates

Syntax	certificates local <i>certificate-name</i> ;
Hierarchy Level	[edit security]
Description	Name of file that contains the pair certificate and private key.
Usage Guidelines	See “Configure JUNOScript XML-SSL Service” on page 360.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

dh-group

Syntax	dh-group (group1 group2);
Hierarchy Level	[edit security ike], [edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the IKE Diffie-Hellman group.
Options	dh-group—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. The dh group can be one of the following: <ul style="list-style-type: none"> ■ group1—768 bit. ■ group2—1,024-bit.
Usage Guidelines	See “Configure an IKE Diffie-Hellman Group” on page 346.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

direction

Syntax	direction (inbound outbound bidirectional);
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual]
Description	Define the direction of the SA.
Options	direction—Direction of IPSec processing. inbound—Inbound SA. outbound—Outbound SA. bidirectional—Bidirectional SA.
Usage Guidelines	See “Configure Direction” on page 340.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

dynamic

Syntax	dynamic { security-association (32 64); ipsec-policy <i>ipsec-policy-name</i> ; }
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define a dynamic IPSec SA.
Options	replay-window-size—Antireplay window size. The replay-window-size statement is optional. 32—32-packet window size. 64—64-packet window size. <i>ipsec-policy-name</i> —Name of IPSec policy
Usage Guidelines	See “Configure the ES PIC” on page 354 and “Configure Dynamic Security Associations” on page 343.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

encryption

Syntax encryption {
 algorithm (des-cbc | 3des-cbc);
 key (ascii-text *key* | hexadecimal *key*);
 }

Hierarchy Level [edit security ipsec security-association *name* manual direction (inbound | outbound | bidirectional)]

Description Configure an encryption algorithm and key for manual SA.

Options algorithm—Type of encryption algorithm.

The algorithm can be one of the following:

- des-cbc—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
- 3des-cbc—Has block size of 8 bytes (64 bits); its key size is 192 bits long.



Note

For 3des-cbc, the first 8 bytes must not be same as the second 8 bytes, and the second 8 bytes must not be same as the third 8 bytes.

key—Type of encryption key.

The key can be one of the following:

- ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters.
- hexadecimal—Hexadecimal key. For the des-cbc option, the key contains 16 hexadecimal characters; for the 3des-cbc option, the key contains 48 hexadecimal characters.

Usage Guidelines See “Configure Encryption” on page 342.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

encryption-algorithm

Syntax	encryption-algorithm (3des-cbc des-cbc);
Hierarchy Level	[edit security ike], [edit security ipsec], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure an IKE or IPSec encryption algorithm.
Options	encryption-algorithm—Type of encryption algorithm. The encryption algorithm can be one of the following: <ul style="list-style-type: none"> ■ 3des-cbc—Has block size of 24 bytes; its key size is 192 bits long. ■ des-cbc—Has a block size of 8 bytes; its key size is 48 bits long.
Usage Guidelines	See “Configure an IKE Encryption Algorithm” on page 346 and “Configure an Encryption Algorithm” on page 350.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

ike

Syntax	ike { proposal <i>ike-proposal-name</i> { authentication-algorithm (md5 sha1); authentication-method pre-shared-keys; dh-group (group1 group2); encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i> ; } policy <i>ike-peer-address</i> { mode (aggressive main); proposal [<i>ike-proposal-names</i>]; pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); } }
Hierarchy Level	[edit security]
Description	Configure IKE. The statements are explained separately.
Usage Guidelines	See “Configure IKE (Dynamic SAs Only)” on page 344.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ipsec

```

Syntax  ipsec {
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol esp;
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposal [ipsec-proposal-names];
    }
    security-association name {
        mode (tunnel | transport);
        manual {
            direction (inbound | outbound | bi-directional) {
                spi spi-value;
                protocol (esp | ah);
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
            }
            dynamic {
                replay-window-size (32 | 64);
                ipsec-policy policy-name;
            }
        }
    }
}

```

Hierarchy Level [edit security]

Description Configure IPSec.

The statements are explained separately.

Usage Guidelines See “Configure Global IPSec Properties” on page 336.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

lifetime-seconds

Syntax	lifetime-seconds <i>seconds</i> ;
Hierarchy Level	[edit security ike], [edit security ipsec], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	(Optional) Configure lifetime of IKE or IPSec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.
Options	<i>seconds</i> —lifetime in seconds. Range: 180 through 86,400
Usage Guidelines	See “Configure IKE Lifetime” on page 346 and “Configure IPSec Lifetime” on page 351.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

manual

Syntax	<pre> manual { direction (inbound outbound bi-directional) { spi <i>spi-value</i>; protocol (esp ah); authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } } } </pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define a manual IPSec SA. The remaining statements are explained separately.
Usage Guidelines	See “Configure Manual Security Associations” on page 339.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

mode

mode (IPSec)

Syntax	mode (transport tunnel);
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define the mode for the IPSec security association.
Options	<p>mode—Type of IPSec protection.</p> <p>transport—Protects host-to-host connections.</p> <p>tunnel—Protects traffic traveling between two security gateways.</p> <p>Default: tunnel</p>



Note

Tunnel mode requires the ES PIC.

The JUNOS software supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the JUNOS software does not support AH and ESP header bundles.

Usage Guidelines	See “Configure IPSec Mode” on page 338.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

mode (IKE)

Syntax	mode (aggressive main);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define IKE policy mode.
Options	<p>mode—Type of IKE policy.</p> <p>aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection.</p> <p>main—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.</p> <p>Default: main</p>
Usage Guidelines	See “Configure IKE Policy Mode” on page 348.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

perfect-forward-secrecy

Syntax perfect-forward-secrecy {
 keys (group1 | group2);
}

Hierarchy Level [edit security ipsec policy *ipsec-policy-name*]

Description (Optional) Define Perfect Forward Secrecy (PFS). Creates single use keys.

Options keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.

The key can be one of the following:

■ group1—768-bit.

■ group2—1,024-bit.

Usage Guidelines See “Configure Perfect Forward Secrecy” on page 352.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

policy

policy (IPSec)

Syntax policy *ipsec-policy-name* {
 perfect-forward-secrecy {
 keys (group1 | group2);
 }
 proposal [*ipsec-proposal-names*];
}

Hierarchy Level [edit security ipsec]

Description Define an IPSec policy.

Options *ipsec-policy-name*—Specifies a IPSec policy name.

proposal—Lists proposals to be used by the IPSec policy.

The remaining statements are explained separately.

Usage Guidelines See “Configure an IPSec Policy” on page 352.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

policy (IKE)

Syntax	<pre>policy <i>ike-peer-address</i> { mode (aggressive main); proposal [<i>ike-proposal-names</i>]; pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); }</pre>
Hierarchy Level	[edit security ike]
Description	Define an IKE policy.
Options	<p><i>ike-peer-address</i>—A tunnel address configured at the [edit interfaces <i>es</i>] hierarchy level.</p> <p><i>proposal</i>—Lists proposals to be used by IKE policy.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configure an IKE Policy” on page 347.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

pre-shared-key

Syntax	pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define a preshared key for an IKE policy.
Options	<p>preshared-key—Type of preshared key.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none"> ■ ascii-text—ASCII text key. ■ hexadecimal—Hexadecimal key. <p>The preshared key can be an ACSII text or hexadecimal character key.</p>
Usage Guidelines	See “Configure IKE Policy Preshared Key” on page 348.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

proposal

proposal (IKE)

Syntax	<pre>proposal <i>ike-proposal-name</i> { authentication-algorithm (md5 sha1); authentication-method pre-shared-keys; dh-group (group1 group2); encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i>; }</pre>
Hierarchy Level	[edit security ike]
Description	Define an IKE proposal for a dynamic SA.
Options	<p><i>ike-proposal-name</i>—Specifies a IKE proposal name</p> <p>The statements are explained separately.</p>
Usage Guidelines	See “Configure an IPSec Proposal” on page 350.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

proposal (IPSec)

Syntax	<pre>proposal <i>ipsec-proposal-name</i> { authentication-algorithm (hmac-md5-96 hmac-sha1-96); encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i>; protocol esp; }</pre>
Hierarchy Level	[edit security ipsec]
Description	Define an IPSec proposal for a dynamic SA.
Options	<p><i>ipsec-proposal-name</i>—Specifies an IPSec proposal name.</p> <p>The statements are explained separately.</p>
Usage Guidelines	See “Configure an IPSec Proposal” on page 350.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

protocol

protocol (manual SA)

Syntax	protocol (esp ah);
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bidirectional)]
Description	Define an IPSec protocol for a manual SA.
Options	protocol—Type of IPSec protocol The protocol can be one of the following: esp—Encapsulating security payload protocol. ah—Authentication header protocol.
Usage Guidelines	See “Configure the Protocol” on page 341.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

protocol (dynamic SA)

Syntax	protocol esp;
Hierarchy Level	[edit security ipsec], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Define an IPSec protocol for a dynamic SA.
Options	esp—Encapsulating security payload (the tunnel statement must be included at the [edit security ipsec security-association <i>name</i> mode] hierarchy level).

**Note**

The JUNOS software does not support the Authentication Header protocol in tunnel mode.

Usage Guidelines	See “Configure Protocol for Dynamic SA” on page 351.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

security-association

```

Syntax security-association name {
    mode (tunnel | transport);
    manual {
        direction (inbound | outbound | bi-directional) {
            spi spi-value;
            protocol (esp | ah);
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key);
            }
            encryption {
                algorithm (des-cbc | 3des-cbc);
                key (ascii-text key | hexadecimal key);
            }
        }
        dynamic {
            replay-window-size (32 | 64);
            ipsec-policy policy-name;
        }
    }
}

```

Hierarchy Level [edit security ipsec]

Options *name*—Name of security association

The remaining statements are explained separately.

Description Configure an IPSec security association.

Usage Guidelines See “Configure Security Associations” on page 337.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

spi

Syntax spi *spi-value*;

Hierarchy Level [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional)]

Description Configure Security Parameter Index (SPI) for an SA.

Options *spi-value*—An arbitrary value that uniquely identifies which security association (SA) to use at the receiving host (the destination address in the packet).
Range: 256 through 16, 639

Usage Guidelines See “Configure a Security Parameter Index (SPI)” on page 341.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

traceoptions

Syntax	<pre>[edit security] traceoptions { file <files number> <size size>; flag all; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; }</pre>
Hierarchy Level	[edit security]
Description	<p>Configure security tracing options.</p> <p>To specify more than one tracing option, include multiple flag statements. The output of the security tracing options is placed in one file: /var/log/kmd.</p>
Options	<p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>size <i>size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, kmd) reaches this size, it is renamed, kmd.0, then kmd.1 and so on., until the maximum number of trace files is reached. Then the oldest trace file is overwritten. Default: 1024 KB</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option: Range: 2 through 1,000 files Default: 10 files</p> <p>flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <ul style="list-style-type: none"> ■ all—Trace all security event ■ database—Trace database events ■ general—Trace general events ■ ike—Trace IKE module processing ■ parse—Trace configuration processing ■ policy-manager—Trace policy manager processing ■ routing-socket—Trace routing socket messages ■ timer—Trace internal timer events

• Usage Guidelines	See “Configure Traceoptions” on page 354
•	
• Required Privilege Level	admin—To view the in the configuration.
•	admin-control—To add this statement to the configuration.

Part 7

Router Chassis

- Router Chassis Configuration Guidelines on page 379
- Summary of Router Chassis Configuration Statements on page 397



Chapter 30

Router Chassis Configuration Guidelines

You can configure properties of the router chassis, including the clock source, conditions that activate the red and yellow alarm light-emitting diodes (LEDs) on the router's craft interface, and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs).

To configure router chassis properties, you include statements at the [edit chassis] hierarchy level of the configuration:

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
    sonet {
      device-count number;
    }
  }
  alarm {
    interface-type {
      alarm-name (red | yellow | ignore);
    }
  }
  fpc slot-number {
    pic pic-number {
      atm-cell-relay-accumulation;
      ce1 {
        e1 port-number {
          channel-group group-number timeslots slot-number;
        }
      }
      ct3 {
        port port-number {
          t1 link-number {
            channel-group group-number timeslots slot-number;
          }
        }
      }
    }
    framing (sdh | sonet);
    no-concatenate;
    sparse-dlcis;
    vtmapping (itu-t | klm);
  }
}
```

```

(packet-scheduling | no-packet-scheduling);
(source-route | no-source-route);
redundancy {
    failover on-loss-of keepalives on-loss-of-keepalives;
    keepalive-time seconds;
    routing-engine slot-number (master | backup | disabled);
    sfm slot-number (always | preferred);
    ssb slot-number (always | preferred);
}
}

```

This chapter describes the following tasks for configuring the router chassis:

- Minimum Chassis Configuration on page 380
- Configure Aggregated Devices on page 381
- Configure ATM Cell-Relay Accumulation Mode on page 381
- Configure Conditions That Trigger Alarms on page 382
- Configure SONET/SDH Framing on page 384
- Configure Sparse DLCIS Mode on page 385
- Configure Channelized PIC Operation on page 385
- Channelized DS-3 to DS-0 Naming on page 386
- Channelized E1 Naming on page 388
- Channelized STM-1 Interface Virtual Tributary Mapping on page 389
- Configure the Drop Policy for Traffic with Source-Route Constraints on page 390
- Configure Redundancy on page 390
- Configure Packet Scheduling on page 395

Minimum Chassis Configuration

All the statements at the [edit chassis] hierarchy level of the configuration are optional.

Configure Aggregated Devices

JUNOS software supports the aggregation of physical devices into defined virtual links, such as the link aggregation of Ethernet interfaces defined by the IEEE 802.3ad standard. To define the virtual links, you need to specify the associations between physical and logical devices within the [edit interfaces] hierarchy, and assign the correct number of logical devices by including the device-count statement at the [edit chassis aggregated-devices ethernet] and [edit chassis aggregated-devices sonet] hierarchy levels:

```
[edit chassis]
aggregated-devices {
  ethernet {
    device-count 16;
  }
  sonet {
    device-count 16;
  }
}
```

The maximum number of logical devices you can assign is 16. For more information on physical and logical interfaces using aggregated links, including sample configurations, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Configure ATM Cell-Relay Accumulation Mode

You can configure an ATM PIC to use cell-relay accumulation mode. In this mode, the incoming cells (1 to 8 cells) are packaged into a single packet and forwarded to the label-switched path (LSP). At the edge router, this packet is divided into individual cells and transmitted over the ATM interface.



When you configure an ATM PIC to use cell-relay accumulation, all ports on the ATM PIC use cell-relay accumulation mode.

To configure an ATM PIC to use cell-relay accumulation mode, include the atm-cell-relay-accumulation statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
atm-cell-relay-accumulation;
```

Configure Conditions That Trigger Alarms

For the different types of PICs, you can configure which conditions trigger alarms and whether they trigger a red or yellow alarm, or are ignored. Red alarm conditions light the RED ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the contacts on the craft interface. Yellow alarm conditions light the YELLOW ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the craft interface.

To configure conditions that trigger alarms and that can occur on any interface of the specified type, include the alarm statement at the [edit chassis] hierarchy level:

```
[edit chassis]
alarm {
  interface-type {
    alarm-name (red | yellow | ignore);
  }
}
```

alarm-name is the name of an alarm. Table 17 lists the systemwide alarms and the alarms for each interface type.

Table 17: Configurable PIC Alarm Conditions

Interface/System	Alarm Condition	Configuration Option
SONET/SDH and ATM	Link alarm indication signal	ais-l
	Path alarm indication signal	ais-p
	Signal degrade (SD)	ber-sd
	Signal fail (SF)	ber-sf
	Loss of cell delineation (ATM only)	locd
	Loss of framing	lof
	Loss of light	lol
	Loss of pointer	lop-p
	Loss of signal	los
	Phase locked loop out of lock	pll
	STS payload label (C2) mismatch	plm-p
	Line remote failure indication	rfl-l
	Path remote failure indication	rfl-p
	STS path (C2) unequipped	uneq-p

Interface/System	Alarm Condition	Configuration Option
E3/T3	Alarm indicator signal	ais
	Excessive numbers of zeros	exz
	Failure of the far end	ferf
	Idle alarm	idle
	Line code violation	lcv
	Loss of frame	lof
	Loss of signal	los
	Phase locked loop out of lock	pll
	Yellow alarm	ylw
Ethernet	Link has gone down	link-down
DS-1	Alarm indicator signal	ais
	Yellow alarm	ylw
Management-Ethernet	Link has gone down	link-down

Chassis Conditions That Trigger Alarms

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. Table 18 lists the alarms that the chassis components can generate.

Table 18: Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Alarm Severity
Alternative Media	Router boots from alternate boot device. For more information about alternate boot devices, see "Boot Devices" on page 78.	Yellow
Fans	One fan has been removed from the chassis.	Yellow
	Two or more fans have been removed from the chassis.	Red
	One fan in the chassis is installed but not spinning.	Red
Power supplies	A power supply has been removed from the chassis.	Yellow
	A power supply has failed. If both power supplies fail, the router shuts down and the software might report the failures in the syslog file.	Red
Temperature	Chassis temperature has exceeded 54 degrees Centigrade and the fans have been turned on to full speed.	Yellow
	Chassis temperature has exceeded 75 degrees Centigrade and the router has been shut down.	Red
	The temperature sensor has failed.	Red
SCB/SSB/FEB/SFM	The control board (SCB, SSB, FEB, or SFM, depending on model) has failed. If this occurs, the board attempts to reboot.	Red

Chassis Component	Alarm Condition	Alarm Severity
FPC	An FPC has failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Red
Craft interface	The craft interface has failed.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	Red

Silence External Devices

You can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button located on the craft interface front panel. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after an external device is silenced reactivate the external device.

Configure SONET/SDH Framing

By default, SONET/SDH PICs use SONET framing. For a discussion of the differences between the two standards, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*. To configure a PIC to use SDH framing, include the framing statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level, specifying the sdh option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sdh
[edit chassis]
user@host# show
fpc slot-number {
    pic pic-number {
        framing sdh;
    }
}
```

To explicitly configure a PIC to use SONET framing, include the framing statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level, specifying the sonet option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis]
user@host# show
fpc slot-number {
    pic pic-number
        framing sonet;
    }
}
```

Configure Sparse DLCIS Mode

By default, Channelized DS-3 and Channelized STM1 to E1 (or T1) interfaces can support a maximum of 64 data-link connection identifiers (DLCIs) per channel—as many as 1,792 DLCIs per DS-3 interface or 4,032 DLCIs per STM1 interface (0 through 63).

In sparse DLCIS mode, the full DLCI range (1 through 1,022) is supported. This allows you to use circuit cross-connect (CCC) and translation cross connect (TCC) features by means of Frame Relay on T1 and E1 interfaces. For more information about CCC and DLCIs, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.



Note

Sparse DLCIS mode requires a Channelized STM1 or Channelized DS-3 PIC.

DLCI 0 is reserved for LMI signaling.

To configure the router to use sparse DLCIS mode, include the `sparse-dlcis` statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
sparse-dlcis;
```

Configure Channelized PIC Operation

By default, packet-over-SONET PICs (interfaces with names `so-fpc/pic/port`) operate in concatenated mode, a mode in which the bandwidth of the interface is in a single channel. To configure a PIC to operate in channelized (multiplexed) mode, include the `no-concatenate` statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number no-concatenate
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number
  no-concatenate;
}
```

When configuring and displaying information about interfaces that are operating in channelized mode, you must specify the channel number in the interface name (*physical:channel*); for example, `so-2/2/0:0` and `so-2/2/0:1`. For more information about interface names, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Concatenated and Nonconcatenated Mode

On SONET OC-48 interfaces that are configured for channelized (multiplexed) mode, the bytes e1-quiet and bytes f1 options in the sonet-options statement have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0. These bytes work in the transmit direction only on channels 1, 2, and 3.

The M160 four-port POS OC-12 PIC can run each of the OC-12 links in concatenated mode only and requires a Type 2 M160 Flexible PIC Concentrator (FPC). Similarly, the four-port POS OC-3 PIC cannot run in nonconcatenated mode on any platform.

Channelized DS-3 to DS-0 Naming

You can configure 28 T1 channels per T3 interface. Each T1 link can have up to eight channel groups, and each channel group can hold any combination of DS-0 timeslots. To specify the T1 link and DS-0 channel group number in the name, use colons (:) as separators. For example, a Channelized DS-3 to DS-0 PIC might have the following physical and virtual interfaces:

```
ds-0/0/0:x:y
```

where *x* is a T1 link ranging from 0 through 27 and *y* is a DS-0 channel group ranging from 0 through 7 (see Table 19, “Ranges for Channelized DS-3 to DS-0 Configuration” on page 387 for more information about ranges).

You can use any of the values within the range available for *x* and *y*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

- You can configure t3-options for t1 link 0 and channel group 0 only; for example, ds-0/0/0:0:0.
- You can configure t1-options for any t1 link value, but only for channel group 0; for example, ds-0/0/0:x:0.
- There are no restrictions on changing the default ds0-options.
- If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and timeslots for a Channelized DS-3 interface, include the channel-group and timeslots statements at the [edit chassis fpc slot-number pic *pic-number* ct3 port *port-number* t1 *link-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
  fpc slot-number {
    pic pic-number {
      ct3 {
        port port-number {
          t1 link-number {
            channel-group group-number timeslots slot-number;
          }
        }
      }
    }
  }
```



If you commit the interface name but do not include the [edit chassis] configuration, the Channelized DS-3 to DS-0 PIC behaves like a Channelized DS-3 to DS-1 PIC: none of the DS-0 functionality is accessible.

Table 19 shows the ranges for each of the quantities in the preceding configuration.

Table 19: Ranges for Channelized DS-3 to DS-0 Configuration

Item	Variable	Range
FPC slot	<i>slot-number</i>	0 through 7 (see note below)
PIC slot	<i>pic-number</i>	0 through 3
Port	<i>port-number</i>	0 through 1
T1 link	<i>link-number</i>	0 through 27
DS-0 channel group	<i>group-number</i>	0 through 7
timeslot	<i>slot-number</i>	1 through 24



FPC slot range depends on platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. (The Multichannel DS-3 (Channelized DS-3 to DS-0) PIC is not supported on M160 routers.)

Bandwidth limitations restrict the interface to a maximum of 128 channel groups per T3 port, rather than the theoretical maximum of $8 \times 28 = 224$.

There are 24 timeslots on a T1 interface. You can designate any combination of timeslots for usage, but you can use each timeslot number on only one channel group within the same T1 link.

To use timeslots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-10;
```

To use timeslots 1 through 5, timeslot 10, and timeslot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify timeslot numbers. For further information on these interfaces, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Channelized E1 Naming

Each Channelized E1 PIC has 10 E1 ports that you can channelize to the *NxDS-0* level. Each E1 interface has 32 timeslots (DS-0), in which timeslot 0 is reserved. You can combine one or more of these DS-0 (channels) to create a channel group (*NxDS-0*). There can be a maximum of 24 channel groups per E1 interface. Thus, you can configure as many as 240 channel groups per PIC (10 ports x 24 channel groups per port).

To specify the DS-0 channel group number in the interface name, include a colon (:) as a separator. For example, a Channelized E1 PIC might have the following physical and virtual interfaces:

`ds-0/0/0:x`

where *x* is a DS-0 channel group ranging from 0 through 23 (see Table 20 on page 389 for more information about ranges).

You can use any of the values within the range available for *x*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

- You can configure the `e1-options` statement for channel group 0 only; for example, `ds-0/0/0:0`.
- There are no restrictions on changing the default `ds0-options`.
- If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and timeslots for a Channelized E1 interface, include the `channel-group` and `timeslots` statements at the `[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
fpc slot-number {
  pic pic-number {
    ce1 {
      e1 port-number {
        channel-group group-number timeslots slot-number;
      }
    }
  }
}
```



Note

If you commit the interface name but do not include the `[edit chassis]` configuration, the Channelized E1 PIC behaves like a standard E1 PIC: none of the DS-0 functionality is accessible.

Table 20 shows the ranges for each of the quantities in the preceding configuration.

Table 20: Ranges for Channelized E1 Configuration

Item	Variable	Range
FPC slot	<i>slot-number</i>	0 through 7 (see note below)
PIC slot	<i>pic-number</i>	0 through 3
E1 port	<i>port-number</i>	0 through 9
DS-0 channel group	<i>group-number</i>	0 through 23
timeslot	<i>slot-number</i>	1 through 32



Note

FPC slot range depends on platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. (The Channelized E1 PIC is not supported on M160 routers.)

The theoretical maximum number of channel groups possible per PIC is $10 \times 24 = 240$. This is within the maximum bandwidth available.

There are 32 timeslots on an E1 interface. You can designate any combination of timeslots for usage.

To use timeslots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-10;
```

To use timeslots 1 through 5, timeslot 10, and timeslot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify timeslot numbers.

For further information about these interfaces, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Channelized STM-1 Interface Virtual Tributary Mapping

You can configure virtual tributary mapping to use KLM or ITU-T mode. To configure virtual tributary mapping, include the *vtmapping* statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

By default, virtual tributary mapping uses KLM mode. For more information, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

Configure the Drop Policy for Traffic with Source-Route Constraints

By default, the router forwards IP traffic that has either loose or strict source-route constraints. However, you might want the router to use only the IP destination address on transit traffic for forwarding decisions. You can configure the router to discard IP traffic with source-route constraints by including the `no-source-route` statement at the [edit chassis] hierarchy level:

```
[edit chassis]
no-source-route;
```

Configure Redundancy

For routers that have multiple Routing Engines or multiple System and Switch Boards (SSBs), you can configure redundancy properties. A separate log file is provided for redundancy logging, located at `/var/log/mastership`.

This section describes the following tasks for configuring redundancy:

- Configure Routing Engine Redundancy on page 390
- Configure SFM Redundancy on page 394
- Configure SSB Redundancy on page 394

For information about how to synchronize Routing Engines, see “Synchronize Routing Engines” on page 160.

Configure Routing Engine Redundancy

For routers with two Routing Engines, you can configure which Routing Engine is the master and which is the backup. By default, the Routing Engine in slot 0 is the master (RE0) and the one in slot 1 is the backup (RE1).

To modify the default configuration, include the `routing-engine` statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
routing-engine slot-number (master | backup | disabled);
```

slot-number can be 0 or 1. To configure the Routing Engine to be the master, specify the `master` option. To configure it to be the backup, specify the `backup` option. To switch between the master and the backup Routing Engines, you must modify the configuration and then activate the configuration by issuing the `commit` command.



For routers that have two Routing Engines, both must be running JUNOS Internet software Release 4.0 or later. Do not run JUNOS Internet software Release 3.4 on one of the Routing Engines and Release 4.0 on the other. (Note that Release 3.4 does not support Routing Engine redundancy, so if you are using this release of the software, only one Routing Engine can be installed in the router. It can be installed in either slot.)

If you have Release 3.4 installed on one of the Routing Engines and Release 4.0 or later on the other, either remove the backup Routing Engine from the router or install Release 4.0 or later on that Routing Engine.



We recommend that both Routing Engines have the same configuration.

You can use either the console port or the management Ethernet (fxp0) port to establish connectivity between the two Routing Engines. You can then copy or ftp the configuration from the master to the backup, and load the file and commit it in the normal way.

To make a tty connection to the other Routing Engine using the router's internal Ethernet network, issue the following command:

```
user@host > request routing-engine login (other-routing-engine | re0 | re1)
```

You can configure Routing Engine redundancy in the following ways:

- Copy a Configuration File from One Routing Engine to the Other on page 391
- Load a Package from the Other Routing Engine on page 393
- Change over to the Backup Routing Engine on page 393

Copy a Configuration File from One Routing Engine to the Other

To copy a configuration file from one Routing Engine to the other, you use the existing file copy command:

```
user@host > file copy source destination
```

In this case, *source* is the name of the configuration file. These files are stored in the directory /config. The active configuration is /config/juniper.conf, and older configurations are in /config/juniper.conf { 1...9 }. *destination* is a file on the other Routing Engine.

The following is an example of copying a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

To load the file into configuration mode, use the load replace configuration mode command:

```
user@host% load replace /var/tmp/copied-juniper.conf
```



Caution

Make sure you change any IP addresses specified in fxp0 on Routing Engine 0 to addresses appropriate for Routing Engine 1.

You can use configuration groups to ensure that the correct IP addresses are used for each Routing Engine and to maintain a single configuration file for both Routing Engines.

The following example defines configuration groups re0 and re1 with separate IP addresses. These well-known configuration group names take effect only on the appropriate Routing Engine.

```
groups {
  re0 {
    system {
      host-name my-re0;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.40/24;
          }
        }
      }
    }
  }
  re1 {
    system {
      host-name my-re1;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.41/24;
          }
        }
      }
    }
  }
}
```

For more information about the configuration groups feature, see “Configuration Groups” on page 179.

Load a Package from the Other Routing Engine

You can load a package from the other Routing Engine onto the local Routing Engine using the existing request system software add *package-name* command:

```
user@host > request system software add re(0|1):/filename
```

In the *re* portion of the URL, specify the number of the other Routing Engine. In the *filename* portion of the URL, specify the path to the package. Packages are typically in the directory */var/sw/pkg*.

Change over to the Backup Routing Engine

Once you have configured a backup Routing Engine, you can direct it to assume mastership automatically if it detects loss of keepalive signal from the master. By default, this feature is disabled; to enable it, include the failover on-loss-of-keepalives statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
failover on-loss-of keepalives on-loss-of-keepalives;
```

By default, failover will occur after 300 seconds (5 minutes). To change the keepalive time period, include the keepalive-time statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
keepalive-time seconds;
```

The range for keepalive-time is 2 through 10,000 seconds.

If you configure the keepalive time for 2 seconds, the sequence of events is as follows:

1. After 2 seconds of keepalive loss, a message is logged.
2. After 2 seconds of keepalive loss, the backup Routing Engine attempts to assume mastership. An alarm is generated whenever the backup is active and the display is updated with current status.
3. Once the backup Routing Engine assumes mastership, it continues to function as master even after the originally configured master Routing Engine has successfully resumed operation. You must intervene to restore its previous backup status. However, if at any time one of the Routing Engines is not present, the other one becomes master automatically, regardless of how redundancy is configured.

Configure SFM Redundancy

For routers with two Switching and Forwarding Modules (SFM), you can configure which SFM is the master and which is the backup. By default, the SFM in slot 0 is the master and the one in slot 1 is the backup. To modify the default configuration, include the `sfm` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
sfm slot-number (always | preferred);
```

`slot-number` can be 0 or 1.

`always` defines the SFM as the sole device.

`preferred` defines a preferred SFM.



SFM redundancy is for M40e routers only.

Configure SSB Redundancy

For routers with two System and Switch Boards (SSB), you can configure which SSB is the master and which is the backup. By default, the SSB in slot 0 is the master and the one in slot 1 is the backup. To modify the default configuration, include the `ssb` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
ssb slot-number (always | preferred);
```

`slot-number` can be 0 or 1.

`always` defines the `ssb` as the sole device.

`preferred` defines a preferred `ssb`.



SSB redundancy is for M20 routers only.

Configure Packet Scheduling

Packet scheduling is for M160 routers only. By default, packet scheduling is disabled. To configure a router to operate in packet-scheduling mode, include the packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
packet-scheduling;
```

To explicitly disable the packet-scheduling statement, include the no-packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
no-packet-scheduling;
```

When you enable packet-scheduling mode, the Packet Director ASIC schedules packet dispatches to compensate for transport delay differences. This preserves the interpacket gaps as the packets are distributed from the Packet Director ASIC to the Packet Forwarding Engine.

Whenever you change the configuration for packet-scheduling, the system stops all Switching and Forwarding Modules (SFMs) and Flexible Pic Concentrators (FPCs) and restarts them in the new mode.

Chapter 31

Summary of Router Chassis Configuration Statements

The following sections explain each of the chassis configuration statements. The statements are organized alphabetically.

aggregated-devices

Syntax	<pre>aggregated-devices { ethernet { device-count <i>number</i>; } sonet { device-count <i>number</i>; } }</pre>
Hierarchy Level	[edit chassis]
Description	Configure properties for aggregated devices on the router.
Options	The statements are explained separately in this chapter.
Usage Guidelines	See “Configure Aggregated Devices” on page 381.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

alarm

Syntax alarm {
 interface-type {
 alarm-name (red | yellow | ignore);
 }
 }

Hierarchy Level [edit chassis]

Description Configure the chassis alarms and whether they trigger a red or yellow alarm, or whether they are ignored. Red alarm conditions light the RED ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the contact on the craft interface. Yellow alarm conditions light the YELLOW ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the craft interface.

To configure more than one alarm, include multiple *alarm-name* lines.

Options *alarm-name*—Alarm condition. For a list of conditions, see Table 17 on page 382.

ignore—The specified alarm condition does not set off any alarm.

interface-type—Type of interface on which you are configuring the alarm. It can be one of the following: atm, ethernet, sonet, or t3.

red—The specified alarm condition sets off a red alarm.

yellow—The specified alarm condition sets off a yellow alarm.

Usage Guidelines See "Chassis Conditions That Trigger Alarms" on page 383.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

atm-cell-relay-accumulation

Syntax atm-cell-relay-accumulation;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Description Configure an ATM PIC in cell-relay accumulation mode.

Usage Guidelines See "Configure ATM Cell-Relay Accumulation Mode" on page 381.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

ce1

Syntax ce1 {
 e1 *port-number* {
 channel-group *group-number* timeslots *slot-number*;
 }
 }

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Description Configure channelized E1 port and channel specifications.

Options *port-number*—Any valid E1 port number on the host system.

The remaining statements are explained separately in this chapter.

Usage Guidelines See “Channelized E1 Naming” on page 388.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

channel-group

Syntax channel-group *group-number*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number*];

[edit chassis fpc *slot-number* pic *pic-number* ce1 e1 *port-number*];

Description Configures the DS-0 channel number.

Options *group-number*—DS-0 channel group
 Range: 0 through 7 for DS-0 naming, and 0 through 23 for E1 naming.

Usage Guidelines See “Channelized DS-3 to DS-0 Naming” on page 386 and “Channelized E1 Naming” on page 388.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

chassis

Syntax chassis { ... }

Hierarchy Level [edit]

Description Configure router chassis properties.

Usage Guidelines See “Router Chassis Configuration Guidelines” on page 379.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

ct3

Syntax ct3 {
 port *port-number* {
 t1 *link-number* {
 channel-group *group-number* timeslots *slot-number*;
 }
 }
 }

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Description Configure channelized T3 port and channel specifications.

Options port *port-number*—Any valid T3 port number on the host system.

t1 *link-number*—T1 link
Range: 0 through 27

The remaining statements are explained separately in this chapter.

Usage Guidelines See “Channelized DS-3 to DS-0 Naming” on page 386.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

device-count

Syntax device-count *number*;

Hierarchy Level [edit chassis aggregated-devices ethernet]

Description Configure number of aggregated logical devices available to the router.

Usage Guidelines See “Configure Aggregated Devices” on page 381.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

e1

Syntax e1 *port-number* {
 channel-group *group-number* timeslots *slot-number*;
 }

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ce1]

Description Configure channelized E1 port number on the PIC.
Range: 0 through 9

Usage Guidelines See “Channelized E1 Naming” on page 388.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

ethernet

Syntax	ethernet { device-count <i>number</i> ; }
Hierarchy Level	[edit chassis aggregated-devices]
Description	Configure properties for Ethernet aggregated devices on the router.
Usage Guidelines	See “Configure Aggregated Devices” on page 381.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

failover on-loss-of keepalives

Syntax	failover on-loss-of-keepalives;
Hierarchy Level	[edit chassis redundancy]
Description	Instruct backup router to assume mastership if it detects loss of keepalive signal.
Usage Guidelines	See “Configure Routing Engine Redundancy” on page 390.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

fpc

Syntax

```
fpc slot-number {
  pic pic-number {
    ce1 {
      e1 port-number {
        channel-group group-number timeslots slot-number;
      }
    }
    ct3 {
      port port-number {
        t1 link-number {
          channel-group group-number timeslots slot-number;
        }
      }
    }
  }
  framing (sdh | sonet);
  no-concatenate;
}
```

Hierarchy Level [edit chassis]

Description Configure properties for the Physical Interface Cards (PICs) in individual Flexible PIC Concentrators (FPCs).

Options *slot-number*—Slot number in which the FPC is installed.
Range: 0 through 7

The remaining statements are explained separately in this chapter.

Usage Guidelines See “Configure SONET/SDH Framing” on page 384 and “Configure Channelized PIC Operation” on page 385.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

framing

Syntax	framing (sdh sonet);
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i>]
Description	On SONET PICs only, configure the framing type.
Options	sdh—SDH framing. sonet—SONET framing. Default: sonet
Usage Guidelines	See “Configure SONET/SDH Framing” on page 384.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

keepalive-time

Syntax	keepalive-time <i>seconds</i> ;
Hierarchy Level	[edit chassis redundancy]
Description	Configure the time period that must elapse before backup router assumes mastership if it detects loss of keepalive signal.
Usage Guidelines	See “Configure Routing Engine Redundancy” on page 390.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

no-concatenate

Syntax	no-concatenate;
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i>]
Description	<p>Do not concatenate (multiplex) the output of a packet-over-SONET PIC (an interface with a name <i>so-fpc/pic/port</i>).</p> <p>When configuring and displaying information about interfaces that are operating in channelized mode, you must specify the channel number in the interface name (<i>physical:channel</i>); for example, so-2/2/0:0 and so-2/2/0:1. For more information about interface names, see the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i>.</p> <p>On SONET OC-48 interfaces that are configured for channelized (multiplexed) mode, the bytes e1-quiet and bytes f1 options in the sonet-options statement have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0. They work in the transmit direction only on channels 1, 2, and 3.</p>
Default	Output is concatenated (multiplexed).
Usage Guidelines	See “Configure Channelized PIC Operation” on page 385.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
See Also	<i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .

packet-scheduling

Syntax	(packet-scheduling no-packet-scheduling);
Hierarchy Level	[edit chassis]
Description	<p>Enable packet-scheduling mode, in which the Packet Director ASIC schedules packet dispatches to compensate for transport delay differences. This preserves the interpacket gaps as the packets are distributed from the Packet Director ASIC to the Packet Forwarding Engine.</p>



Note

The packet-scheduling feature is available on M160 routers only.

Options	no-packet-scheduling—Do not schedule packets. packet-scheduling—Schedule packets to preserve interpacket gaps.
Default:	no-packet-scheduling
Usage Guidelines	See “Configure Packet Scheduling” on page 395.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

pic

Syntax

```

pic pic-number {
  ce1 {
    e1 port-number {
      channel-group group-number timeslots slot-number;
    }
  }
  ct3 {
    port port-number {
      t1 link-number {
        channel-group group-number timeslots slot-number;
      }
    }
  }
  framing (sdh | sonet);
  no-concatenate;
}

```

Hierarchy Level [edit chassis *fpc slot-number*]

Description Configure properties for an individual Physical Interface Card (PIC).

Options *pic-number*—Slot number in which the FPC is installed.
Range: 0 through 3

The remaining statements are explained separately in this chapter.

Usage Guidelines See “Configure SONET/SDH Framing” on page 384, “Configure Channelized PIC Operation” on page 385, “Channelized DS-3 to DS-0 Naming” on page 386, and “Channelized E1 Naming” on page 388.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

port

Syntax port *port-number*;

Hierarchy Level [edit chassis *fpc slot-number* pic *pic-number* ct3]

Description Configure channelized T3 port number on the PIC.
Range: 0 through 1

Usage Guidelines See “Channelized DS-3 to DS-0 Naming” on page 386.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

redundancy

Syntax redundancy {
 failover on-loss-of keepalives on-loss-of-keepalives;
 keepalive-time *seconds*;
 routing-engine *slot-number* (backup | disabled | master);
 ssb *slot-number* (always | preferred);
 }

Hierarchy Level [edit chassis]

Description You can configure a redundant Routing Engine or System and Switch Board (SSB) in the chassis as a secondary backup for the chassis. By default, the Routing Engine in slot 0 is the master Routing Engine and the Routing Engine in slot 1 is the backup Routing Engine. The switchover from the master Routing Engine to the backup Routing Engine is performed manually. This feature can be used for software upgrades. New software can be loaded on the backup Routing Engine and when the routing engine is ready, you can switch the mastership over, with a brief interruption in traffic.

Default Slot 0 is preferred.

Options The statements are explained separately.

Usage Guidelines See “Configure Redundancy” on page 390.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

routing-engine

Syntax routing-engine *slot-number* (backup | disabled | master);

Hierarchy Level [edit chassis redundancy]

Description You can configure a redundant Routing Engine in the chassis as a secondary backup for the chassis. By default, the Routing Engine in slot 0 is the master Routing Engine and the Routing Engine in slot 1 is the backup Routing Engine. The switchover from the master Routing Engine to the backup Routing Engine is performed manually. This feature can be used for software upgrades. New software can be loaded on the backup Routing Engine, and when the routing engine is ready, you can switch the mastership over, with a brief interruption.

Default Slot 0 is preferred.

Options *slot number*—Specify which slot is the master and which is the backup.

master—Routing Engine in specified slot is the master.

backup—Routing Engine in specified slot is the backup.

disabled—Routing Engine in specified slot is disabled.

Usage Guidelines See “Configure Routing Engine Redundancy” on page 390.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

sfm

Syntax	sfm <i>slot-number</i> (always preferred);
Hierarchy Level	[edit chassis redundancy]
Description	For routers with two Switching and Forwarding Modules (SFM), you can configure which is the master and which is the backup. By default, the SFM in slot 0 is the master and the one in slot 1 is the backup.



SFM redundancy is for M40e routers only.

Default	Slot 0 is preferred.
Options	<i>slot number</i> —Specify which slot is the master and which is the backup. <i>always</i> —Defines this SFM as the sole device. <i>preferred</i> —Defines this SFM as the preferred device of at least two.
Usage Guidelines	See “Configure SFM Redundancy” on page 394.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

sonet

Syntax	sonet { device-count <i>number</i> ; }
Hierarchy Level	[edit chassis aggregated-devices]
Description	Configure properties for SONET aggregated devices on the router.
Usage Guidelines	See “Configure Aggregated Devices” on page 381.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-route

Syntax	(source-route no-source-route);
Hierarchy Level	[edit chassis]
Description	Configure whether IP traffic with source-route constraints (loose or strict) is forwarded or discarded.
Options	no-source-route—Discard IP traffic that has loose or strict source-route constraints. Use this option when you want the router to use only the IP destination address on transit traffic for forwarding decisions. source-route—Forward IP traffic that has loose or strict source-route constraints.
Default:	source-route
Usage Guidelines	See “Configure the Drop Policy for Traffic with Source-Route Constraints” on page 390.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ssb

Syntax	ssb <i>slot-number</i> (always preferred);
Hierarchy Level	[edit chassis redundancy]
Description	For routers with two System and Switch Boards (SSBs), you can configure which is the master and which is the backup. By default, the SSB in slot 0 is the master and the one in slot 1 is the backup.
Default	Slot 0 is preferred.
Options	<i>slot number</i> —Specify which slot is the master and which is the backup. always—Defines this SSB as the sole device. preferred—Defines this SSB as the preferred device of at least two.
Usage Guidelines	See “Configure SSB Redundancy” on page 394.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

sparse-dlcis

Syntax	sparse-dlcis;
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i>];
Description	Supports full DLCI range (1 through 1,022). This allows you to use circuit cross-connect (CCC) and translation cross connect (TCC) features by means of Frame Relay on T1 and E1 interfaces.
Usage Guidelines	See “Configure Sparse DLCIS Mode” on page 385.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

t1

Syntax	t1 <i>link-number</i> { channel-group <i>group-number</i> timeslots <i>slot-number</i> ; }
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> ct3 port <i>port-number</i>];
Description	Configure channelized T1 port and channel specifications.
Options	<i>link-number</i> —T1 link Range: 0 through 27 for DS-0 Naming The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Channelized DS-3 to DS-0 Naming” on page 386.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

timeslots

Syntax	timeslots <i>slot-number</i>
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> ct3 port <i>port-number</i> t1 <i>link-number</i>]; [edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> ce1 e1 <i>port-number</i>];
Description	For E1 or T1 interfaces, allocate the specific timeslots by number.
Options	<i>slot-number</i> —Actual timeslot number(s) allocated: Range: 1 through 24 for T1 and 1 through 32 for E1. Default: All timeslots for T1 and all timeslots for E1.
Usage Guidelines	See “Channelized DS-3 to DS-0 Naming” on page 386 and “Channelized E1 Naming” on page 388.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

vtmapping

Syntax vtmapping (klm | itu-t);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Description Configure virtual tributary mapping.

Options klm—KLM standard

itu-t—International Telephony Union standard

Default: klm

Usage Guidelines See “Channelized STM-1 Interface Virtual Tributary Mapping” on page 389.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Part 8

Appendix

■ Glossary on page 413

.....

Appendix A

Glossary

A

AAL	ATM adaptation layer. A series of protocols enabling various types of traffic, including voice, data, image, and video, to run over an ATM network.
active route	Route chosen from all routes in the routing table to reach a destination. Active routes are installed into the forwarding table.
add/drop multiplexer	<i>See ADM.</i>
Address Resolution Protocol	<i>See ARP.</i>
adjacency	Portion of the local routing information that pertains to the reachability of a single neighbor over a single circuit or interface.
ADM	Add/drop multiplexer. SONET functionality that allows lower-level signals to be dropped from a high-speed optical connection.
aggregation	Combination of groups of routes that have common addresses into a single entry in the routing table.
AH	Authentication Header. A component of the IPSec protocol used to verify that the contents of a packet have not been changed, and to validate the identity of the sender. <i>See also ESP.</i>
ANSI	American National Standards Institute. The United States' representative to the ISO.
APQ	Alternate Priority Queuing. Dequeuing method that has a special queue, similar to SPQ, which is visited only 50 percent of the time. The packets in the special queue still have a predictable latency, although the upper limit of the delay is higher than that with SPQ. Since the other configured queues share the remaining 50 percent of the service time, queue starvation is usually avoided. <i>See also SPQ.</i>
APS	Automatic Protection Switching. Technology used by SONET ADMs to protect against circuit faults between the ADM and a router and to protect against failing routers.
area	Routing subdomain that maintains detailed routing information about its own internal composition and that maintains routing information that allows it to reach other routing subdomains. In IS-IS, an area corresponds to a Level 1 subdomain. In IS-IS and OSPF, a set of contiguous networks and hosts within an autonomous system that have been administratively grouped together.
area border router	Router that belongs to more than one area. Used in OSPF.

ARP	Address Resolution Protocol. Protocol for mapping IP addresses to MAC addresses.
AS	Autonomous system. Set of routers under a single technical administration. Each AS normally uses a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routers. Also called <i>routing domain</i> .
AS boundary router	In OSPF, routers that exchange routing information with routers in other ASs.
AS external link advertisements	OSPF link-state advertisement sent by AS boundary routers to describe external routes that they know. These link-state advertisements are flooded throughout the AS (except for stub areas).
AS path	In BGP, the route to a destination. The path consists of the AS numbers of all routers a packet must go through to reach a destination.
ASIC	Application-specific integrated circuit. Specialized processors that perform specific functions on the router.
ATM	Asynchronous Transfer Mode. A high-speed multiplexing and switching method utilizing fixed-length cells of 53 octets to support multiple types of traffic.
atomic	Smallest possible operation. An atomic operation is performed either entirely or not at all. For example, if machine failure prevents a transaction from completing, the system is rolled back to the start of the transaction, with no changes taking place.
Authentication Header	<i>See AH.</i>
Automatic Protection Switching	<i>See APS.</i>
autonomous system	<i>See AS.</i>
autonomous system boundary router	In OSPF, routers that exchange routing information with routers in other ASs.
autonomous system external link advertisements	OSPF link-state advertisement sent by autonomous system boundary routers to describe external routes that they know. These link-state advertisements are flooded throughout the autonomous system (except for stub areas).
autonomous system path	In BGP, the route to a destination. The path consists of the autonomous system numbers of all the routers a packet must pass through to reach a destination.
B	
backbone area	In OSPF, an area that consists of all networks in area ID 0.0.0.0, their attached routers, and all area border routers.
backplane	On an M40 router, component of the Packet Forwarding Engine that distributes power, provides signal connectivity, manages shared memory on FPCs, and passes outgoing data cells to FPCs.
bandwidth	The range of transmission frequencies a network can use, expressed as the difference between the highest and lowest frequencies of a transmission channel. In computer networks, greater bandwidth indicates faster data-transfer rate capacity.
Bellcore	Bell Communications Research. Research and development organization created after the divestiture of the Bell System. It is supported by the regional Bell holding companies (RBHCs), which own the regional Bell operating companies (RBOCs).

BERT	Bit error rate test. A test that can be run on a T3 interface to determine whether it is operating properly.
BGP	Border Gateway Protocol. Exterior gateway protocol used to exchange routing information among routers in different autonomous systems.
bit error rate test	<i>See BERT.</i>
BITS	Building Integrated Timing Source. Dedicated timing source that synchronizes all equipment in a particular building.
Border Gateway Protocol	<i>See BGP.</i>
broadcast	Operation of sending network traffic from one network node to all other network nodes.
bundle	Collection of software that makes up a JUNOS software release.
C	
CB	Control Board. Part of the host subsystem that provides control and monitoring functions for router components.
CCC	Circuit cross-connect. A JUNOS software feature that allows you to configure transparent connections between two circuits, where a circuit can be a Frame Relay DLCI, an ATM VC, a PPP interface, a Cisco HDLC interface, or an MPLS label-switched path (LSP).
CE device	Customer edge device. Router or switch in the customer's network that is connected to a service provider's provider edge (PE) router and participates in a Layer 3 VPN.
CFM	Cubic feet per minute. Measure of air flow in volume per minute.
Challenge Handshake Authentication Protocol	<i>See CHAP.</i>
channel service unit	<i>See CSU/DSU.</i>
CHAP	A protocol that authenticates remote users. CHAP is a server-driven, three-step authentication mechanism that depends on a shared secret password that resides on both the server and the client.
CIDR	Classless interdomain routing. A method of specifying Internet addresses in which you explicitly specify the bits of the address to represent the network address instead of determining this information from the first octet of the address.
CIP	Connector Interface Panel. On an M160 router, the panel that contains connectors for the Routing Engines, BITS interfaces, and alarm relay contacts.
circuit cross-connect	<i>See CCC.</i>
class of service	<i>See CoS.</i>
CLEC	(Pronounced "see-lek") Competitive Local Exchange Carrier. Company that competes with the already established local telecommunications business by providing its own network and switching.
CLEI	Common language equipment identifier. Inventory code used to identify and track telecommunications equipment.

CLI	Command-line interface. Interface provided for configuring and monitoring the routing protocol software.
client peer	In a BGP route reflection, a member of a cluster that is not the route reflector. <i>See also nonclient peer.</i>
CLNP	Connectionless Network Protocol. ISO-developed protocol for OSI connectionless network service. CLNP is the OSI equivalent of IP.
cluster	In BGP, a set of routers that have been grouped together. A cluster consists of one system that acts as a route reflector, along with any number of client peers. The client peers receive their route information only from the route reflector system. Routers in a cluster do not need to be fully meshed.
community	In BGP, a group of destinations that share a common property. Community information is included as one of the path attributes in BGP update messages.
confederation	In BGP, a group of systems that appears to external autonomous systems to be a single autonomous system.
constrained path	In traffic engineering, a path determined using RSVP signaling and constrained using CSPF. The ERO carried in the packets contains the constrained path information.
core	The central backbone of the network.
CoS	Class of service. The method of classifying traffic on a packet-by-packet basis using information in the ToS byte to provide different service levels to different traffic.
CPE	Customer premises equipment. Telephone or other service provider equipment located at a customer site.
craft interface	Mechanisms used by a Communication Workers of America craftsperson to operate, administer, and maintain equipment or provision data communications. On a Juniper Networks router, the craft interface allows you to view status and troubleshooting information and perform system control functions.
CSCP	Class Selector Codepoint.
CSNP	Complete sequence number PDU. Packet that contains a complete list of all the LSPs in the IS-IS database.
CSPF	Constrained Shortest Path First. An MPLS algorithm that has been modified to take into account specific restrictions when calculating the shortest path across the network.
CSU/DSU	Channel service unit/data service unit. Channel service unit connects a digital phone line to a multiplexer or other digital signal device. Data service unit connects a DTE to a digital phone line.
customer edge device	<i>See CE device.</i>

D

daemon	Background process that performs operations on behalf of the system software and hardware. Daemons normally start when the system software is booted, and they run as long as the software is running. In the JUNOS software, daemons are also referred to as processes.
damping	Method of reducing the number of update messages sent between BGP peers, thereby reducing the load on these peers without adversely affecting the route convergence time for stable routes.
data circuit-terminating equipment	<i>See DCE.</i>
data-link connection identifier	<i>See DLCI.</i>
data service unit	<i>See CSU/DSU.</i>
Data Terminal Equipment	<i>See DTE.</i>
dcd	The JUNOS software interface process (daemon).
DCE	Data circuit-terminating equipment. RS-232-C device, typically used for a modem or printer, or a network access and packet switching node.
default address	Router address that is used as the source address on unnumbered interfaces.
denial of service	<i>See DoS.</i>
dense wavelength-division multiplexing	<i>See DWDM.</i>
designated router	In OSPF, a router selected by other routers that is responsible for sending link-state advertisements that describe the network, which reduces the amount of network traffic and the size of the routers' topological databases.
destination prefix length	Number of bits of the network address used for host portion of a CIDR IP address.
DHCP	Dynamic Host Configuration Protocol. Allocates IP addresses dynamically so that they can be reused when they are no longer needed.
Diffie-Hellman	A public key scheme, invented by Whitfield Diffie and Martin Hellman, used for sharing a secret key without communicating secret information, thus precluding the need for a secure channel. Once correspondents have computed the secret shared key, they can use it to encrypt communications.
Diffserv	Differentiated Service (based on RFC 2474). Diffserv uses the ToS byte to identify different packet flows on a packet-by-packet basis. Diffserv adds a Class Selector Codepoint (CSCP) and a Differentiated Services Codepoint (DSCP).
Dijkstra algorithm	<i>See SPF.</i>
DIMM	Dual inline memory module. 168-pin memory module that supports 64-bit data transfer.
direct routes	<i>See interface routes.</i>

	DLCI	Data-link connection identifier. Identifier for a Frame Relay virtual connection (also called a logical interface).
	DoS	Denial of service. System security breach in which network services become unavailable to users.
	DRAM	Dynamic random-access memory. Storage source on the router that can be accessed quickly by a process.
	drop profile	Drop probabilities for different levels of buffer fullness that are used by RED to determine from which queue to drop packets.
	DSCP	Differentiated Services Codepoint.
	DSU	Data service unit. A device used to connect a DTE to a digital phone line. Converts digital data from a router to voltages and encoding required by the phone line. <i>See also CSU/DSU.</i>
	DTE	Data Terminal Equipment. RS-232-C interface that a computer uses to exchange information with a serial device.
	DVMRP	Distance Vector Multicast Routing Protocol. Distributed multicast routing protocol that dynamically generates IP multicast delivery trees using a technique called reverse path multicasting (RPM) to forward multicast traffic to downstream interfaces.
	DWDM	Dense wavelength-division multiplexing. Technology that enables data from different sources to be carried together on an optical fiber, with each signal carried on its own separate wavelength.
	Dynamic Host Configuration Protocol	<i>See DHCP.</i>
E	EBGP	External BGP. BGP configuration in which sessions are established between routers in different ASs.
	ECSA	Exchange Carriers Standards Association. A standards organization created after the divestiture of the Bell System to represent the interests of interexchange carriers.
	edge router	In MPLS, a router located at the beginning or end of a label-switching tunnel. When at the beginning of a tunnel, an edge router applies labels to new packets entering the tunnel. When at the end of a tunnel, the edge router removes labels from packets exiting the tunnel. <i>See also MPLS.</i>
	EGP	Exterior gateway protocol, such as BGP.
	egress router	In MPLS, last router in a label-switched path (LSP). <i>See also ingress router.</i>
	EIA	Electronic Industries Association. A United States trade group that represents manufacturers of electronics devices and sets standards and specifications.
	EMI	Electromagnetic interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics or electrical equipment.
	encapsulating security payload	<i>See ESP.</i>
	end system	In IS-IS, network entity that sends and receives packets.

ERO	Explicit Route Object. Extension to RSVP that allows an RSVP PATH message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.
ESP	Encapsulating security payload. A fundamental component of IPSec-compliant VPNs, ESP specifies an IP packet's encryption, data integrity checks, and sender authentication, which are added as a header to the IP packet. <i>See also AH.</i>
explicit path	<i>See signaled path.</i>
Explicit Route Object	<i>See ERO.</i>
export	To place routes from the routing table into a routing protocol.
external BGP	<i>See EBGP.</i>
external metric	A cost included in a route when OSPF exports route information from external autonomous systems. There are two types of external metrics: Type 1 and Type 2. Type 1 external metrics are equivalent to the link-state metric; that is, the cost of the route, used in the internal autonomous system. Type 2 external metrics are greater than the cost of any path internal to the autonomous system.
F	fast reroute Mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.
	FEAC Far-end alarm and control. T3 signal used to send alarm or status information from the far-end terminal back to the near-end terminal and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.
	FEB Forwarding Engine Board. In M5 and M10 routers, provides route lookup, filtering, and switching to the destination port.
	firewall A security gateway positioned between two different networks, usually between a trusted network and the Internet. A firewall ensures that all traffic that crosses it conforms to the organization's security policy. Firewalls track and control communications, deciding whether to pass, reject, discard, encrypt, or log them. Firewalls also can be used to secure sensitive portions of a local network.
	FIFO First in, first out.
	flap damping <i>See damping.</i>
	flapping <i>See route flapping.</i>
	Flexible PIC Concentrator <i>See FPC.</i>
	Forwarding Engine Board <i>See FEB.</i>
	forwarding information base <i>See forwarding table.</i>
forwarding table	JUNOS software forwarding information base (FIB). The JUNOS routing protocol process installs active routes from its routing tables into the Routing Engine forwarding table. The kernel copies this forwarding table into the Packet Forwarding Engine, which is responsible for determining which interface transmits the packets.

FPC Flexible PIC Concentrator. An interface concentrator on which PICs are mounted. An FPC inserts into a slot in a Juniper Networks router. *See also PIC.*

FRU Field-replaceable unit. Router component that customers can replace onsite.

G

group A collection of related BGP peers.

H

hash A one-way function that takes a message of any length and produces a fixed-length digest. In security, a message digest is used to validate that the contents of a message have not been altered in transit. The Secure Hash Algorithm (SHA-1) and Message Digest 5 (MD5) are commonly used hashes.

Hashed Message Authentication Code *See HMAC.*

HDLC High-level data link control. An International Telecommunication Union (ITU) standard for a bit-oriented data link layer protocol on which most other bit-oriented protocols are based.

HMAC Hashed Message Authentication Code. A mechanism for message authentication that uses cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function—for example, MD5 or SHA-1—in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

hold time Maximum number of seconds allowed to elapse between the time a BGP system receives successive keepalive or update messages from a peer.

host module On an M160 router, provides routing and system management functions of the router. Consists of the Routing Engine and Miscellaneous Control Subsystem (MCS).

host subsystem Provides routing and system-management functions of the router. Consists of a Routing Engine and an adjacent Control Board (CB).

I

IANA Internet Assigned Numbers Authority. Regulatory group that maintains all assigned and registered Internet numbers, such as IP and multicast addresses. *See also NIC.*

IBGP Internal BGP. BGP configuration in which sessions are established between routers in the same ASs.

ICMP Internet Control Message Protocol. Used in router discovery, ICMP allows router advertisements that enable a host to discover addresses of operating routers on the subnet.

IDE Integrated Drive Electronics. Type of hard disk on the Routing Engine.

IEC International Electrotechnical Commission. *See ISO.*

IEEE Institute of Electronic and Electrical Engineers. International professional society for electrical engineers.

IETF Internet Engineering Task Force. International community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IGMP	Internet Group Membership Protocol. Used with multicast protocols to determine whether group members are present.
IGP	Interior gateway protocol, such as IS-IS, OSPF, and RIP.
IKE	Internet Key Exchange. The key management protocol used in IPSec, IKE combines the ISAKMP and Oakley protocols to create encryption keys and security associations.
import	To install routes from the routing protocols into a routing table.
ingress router	In MPLS, first router in a label-switched path (LSP). <i>See also egress router.</i>
inter-AS routing	Routing of packets among different ASs. <i>See also EBGp.</i>
intercluster reflection	In a BGP route reflection, the redistribution of routing information by a route reflector system to all nonclient peers (BGP peers not in the cluster). <i>See also route reflection.</i>
interface routes	Routes that are in the routing table because an interface has been configured with an IP address. Also called <i>direct routes</i> .
intermediate system	In IS-IS, network entity that sends and receives packets and that can also route packets.
internal BGP	<i>See IBGP.</i>
Internet Key Exchange	<i>See IKE.</i>
Internet Protocol Security	<i>See IPSec.</i>
Internet Security Association and Key Management Protocol	<i>See ISAKMP.</i>
intra-AS routing	The routing of packets within a single AS. <i>See also IBGP.</i>
IP	Internet Protocol. The protocol used for sending data from one point to another on the Internet.
IPSec	Internet Protocol Security. The industry standard for establishing VPNs, IPSec comprises a group of protocols and algorithms that provide authentication and encryption of data across IP-based networks.
ISAKMP	Internet Security Association and Key Management Protocol. A protocol that allows the receiver of a message to obtain a public key and use digital certificates to authenticate the sender's identity. ISAKMP is designed to be key exchange independent; that is, it supports many different key exchanges. <i>See also IKE and Oakley.</i>
IS-IS	Intermediate System-to-Intermediate System protocol. Link-state, interior gateway routing protocol for IP networks that also uses the shortest-path first (SPF) algorithm to determine routes.
ISO	International Organization for Standardization. Worldwide federation of standards bodies that promotes international standardization and publishes international agreements as International Standards.

ISP Internet service provider. Company that provides access to the Internet and related services.

ITU International Telecommunications Union (formerly known as the CCITT). Group supported by the United Nations that makes recommendations and coordinates the development of telecommunications standards for the entire world.

J

jitter Small random variation introduced into the value of a timer to prevent multiple timer expirations from becoming synchronized.

K

kernel forwarding table *See forwarding table.*

L

label In MPLS, 20-bit unsigned integer in the range 0 through 1048575, used to identify a packet traveling along an LSP.

label-switched path (LSP) Sequence of routers that cooperatively perform MPLS operations for a packet stream. The first router in an LSP is called the *ingress router*; and the last router in the path is called the *egress router*. An LSP is a point-to-point, half-duplex connection from the ingress router to the egress router. (The ingress and egress routers cannot be the same router.)

label switching *See MPLS.*

label-switching router *See LSR.*

link Communication path between two neighbors. A link is *up* when communication is possible between the two end points.

link-state PDU (LSP) Packets that contain information about the state of adjacencies to neighboring systems.

local preference Optional BGP path attribute carried in internal BGP update packets that indicates the degree of preference for an external route.

loose In the context of traffic engineering, a path that can use any route or any number of other intermediate (transit) points to reach the next address in the path. (Definition from RFC 791, modified to fit LSPs.)

LSP *See label-switched path (LSP) or link-state PDU (LSP).*

LSR Label-switching router. A router on which MPLS and RSVP are enabled and is thus capable of processing label-switched packets.

M

martian address Network address about which all information is ignored.

mask *See subnet mask.*

MBGP Multiprotocol BGP. An extension to BGP that allows you to connect multicast topologies within and between BGP ASs.

MBone Internet multicast backbone. An interconnected set of subnetworks and routers that support the delivery of IP multicast traffic. The MBone is a virtual network that is layered on top of sections of the physical Internet.

MCS	Miscellaneous Control Subsystem. On an M160 router, provides control and monitoring functions for router components and SONET clocking for the router.
MD5	Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. It is used in AH and ESP. <i>See also SHA-1.</i>
MDRR	Modified Deficit Round Robin. A method for selecting queues to be serviced.
MED	Multiple exit discriminator. Optional BGP path attribute consisting of a metric value that is used to determine the exit point to a destination when all other factors in determining the exit point are equal.
mesh	Network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections between network nodes.
Message Digest 5	<i>See MD5.</i>
MIB	Management Information Base. Definition of an object that can be managed by SNMP.
midplane	Forms the rear of the PIC cage on M5 and M10 routers and the FPC card cage on M20 and M160 routers. Provides data transfer, power distribution, and signal connectivity.
Miscellaneous Control Subsystem	<i>See MCS.</i>
MPLS	Multiprotocol Label Switching. Mechanism for engineering network traffic patterns that functions by assigning to network packets short labels that describe how to forward them through the network. Also called <i>label switching</i> . <i>See also traffic engineering.</i>
MTBF	Mean time between failure. Measure of hardware component reliability.
MTU	Maximum transfer unit. Limit on segment size for a network.
multicast	Operation of sending network traffic from one network node to multiple network nodes.
multicast distribution tree	The data path between the sender (host) and the multicast group member (receiver or listener).
multiprotocol BGP	<i>See MBGP.</i>
Multiprotocol Label Switching	<i>See MPLS.</i>
N	
neighbor	Adjacent system reachable by traversing a single subnetwork. An immediately adjacent router. Also called a <i>peer</i> .
NET	Network entity title. Network address defined by the ISO network architecture and used in CLNS-based networks.
network layer reachability information	<i>See NLRI.</i>
network link advertisement	An OSPF link-state advertisement flooded throughout a single area by designated routers to describe all routers attached to the network.

Network Time Protocol *See NTP.*

NIC Network Information Center. Internet authority responsible for assigning Internet-related numbers, such as IP addresses and autonomous system numbers. *See also IANA.*

NLRI Network layer reachability information. Information that is carried in BGP packets and is used by MBGP.

nonclient peer In a BGP route reflection, a BGP peer that is not a member of a cluster. *See also client peer.*

not-so-stubby area *See NSSA.*

NSAP Network service access point. Connection to a network that is identified by a network address.

n-selector Last byte of an nonclient peer address.

NSSA Not-so-stubby area. In OSPF, a type of stub area in which external routes can be flooded.

NTP Network Time Protocol. Protocol used to synchronize computer clock times on a network.

O

Oakley A key determination protocol based on the Diffie-Hellman algorithm that provides added security, including authentication. Oakley was the key-exchange algorithm mandated for use with the initial version of ISAKMP, although various algorithms can be used. Oakley describes a series of key exchanges called “modes” and details the services provided by each; for example, Perfect Forward Secrecy for keys, identity protection, and authentication. *See also ISAKMP.*

OC Optical Carrier. In SONET, Optical Carrier levels indicate the transmission rate of digital signals on optical fiber.

OSI Open System Interconnection. Standard reference model for how messages are transmitted between two points on a network.

OSPF Open Shortest Path First. A link-state IGP that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the *Dijkstra algorithm*).

P

package A collection of files that make up a JUNOS software component.

Packet Forwarding Engine The architectural portion of the router that processes packets by forwarding them between input and output interfaces.

path attribute Information about a BGP route, such as the route origin, AS path, and next-hop router.

PCI Peripheral Component Interconnect. Standard, high-speed bus for connecting computer peripherals. Used on the Routing Engine.

PCMCIA Personal Computer Memory Card International Association. Industry group that promotes standards for credit card-size memory or I/O devices.

PDU Protocol data unit. IS-IS packets.

PE router Provider edge router. A router in the service provider's network that is connected to a customer edge (CE) device and that participates in a Virtual Private Network (VPN).

PEC	Policing Equivalence Classes. In traffic policing, a set of packets that is treated the same by the packet classifier.
peer	An immediately adjacent router with which a protocol relationship has been established. Also called a <i>neighbor</i> .
Perfect Forward Secrecy	<i>See PFS.</i>
PFE	<i>See Packet Forwarding Engine.</i>
PFS	A condition derived from an encryption system that changes encryption keys often and ensures that no two sets of keys have any relation to each other. The advantage of PFS is that if one set of keys is compromised, only communications using those keys are at risk. An example of a system that uses PFS is Diffie-Hellman.
Physical Interface Card	<i>See PIC.</i>
PIC	Physical Interface Card. A network interface-specific card that can be installed on an FPC in the router.
PIM	Protocol Independent Multicast. A protocol-independent multicast routing protocol. PIM Sparse Mode routes to multicast groups that might span wide-area and interdomain internets. PIM Dense Mode is a flood-and-prune protocol.
PLP	Packet Loss Priority.
PLP bit	Packet Loss Priority bit. Used to identify packets that have experienced congestion or are from a transmission that exceeded a service provider's customer service license agreement. This bit can be used as part of a router's congestion control mechanism and can be set by the interface or by a filter.
policing	Applying rate limits on bandwidth and burst size for traffic on a particular interface.
pop	Removal of the last label, by a router, from a packet as it exits an MPLS domain.
PPP	Point-to-Point Protocol. Link-layer protocol that provides multiprotocol encapsulation. It is used for link-layer and network-layer configuration.
precedence bits	The first three bits in the ToS byte. On a Juniper Networks router, these bits are used to sort or classify individual packets as they arrive at an interface. The classification determines the queue to which the packet is directed upon transmission.
preference	Desirability of a route to become the active route. A route with a lower preference value is more likely to become the active route. The preference is an arbitrary value in the range 0 through 255 that the routing protocol process uses to rank routes received from different protocols, interfaces, or remote systems.
preferred address	On an interface, the default local address used for packets sourced by the local router to destinations on the subnet.
primary address	On an interface, the address used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.
primary interface	Router interface that packets go out when no interface name is specified and when the destination address does not imply a particular outgoing interface.

Protocol-Independent Multicast *See PIM.*

provider edge router *See PE router.*

provider router Router in the service provider's network that does not attach to a customer edge (CE) device.

PSNP Partial sequence number PDU. Packet that contains only a partial list of the LSPs in the IS-IS link-state database.

push Addition of a label or stack of labels, by a router, to a packet as it enters an MPLS domain.

Q

QoS Quality of service. Performance, such as transmission rates and error rates, of a communications channel or system.

quality of service *See QoS.*

R

RADIUS Remote Authentication Dial-In User Service. Authentication method for validating users who attempt to access the router using Telnet.

Random Early Detection *See RED.*

rate limiting *See policing.*

RBOC (Pronounced "are-bock") Regional Bell operating company. Regional telephone companies formed as a result of the divestiture of the Bell System.

RDRAM RAMBUS dynamic random access memory.

RED Random Early Detection. Gradual drop profile for a given class that is used for congestion avoidance. RED tries to anticipate incipient congestion and reacts by dropping a small percentage of packets from the head of the queue to ensure that a queue never actually becomes congested.

Rendezvous Point *See RP.*

Resource Reservation Protocol *See RSVP.*

RFC Request for Comments. Internet standard specifications published by the Internet Engineering Task Force.

RFI Radio frequency interference. Interference from high-frequency electromagnetic waves emanating from electronic devices.

RIP Routing Information Protocol. Distance-vector interior gateway protocol that makes routing decisions based on hop count.

route flapping Situation in which BGP systems send an excessive number of update messages to advertise network reachability information.

route identifier IP address of the router from which a BGP, IGP, or OSPF packet originated.

route reflection	In BGP, configuring a group of routers into a cluster and having one system act as a route reflector, redistributing routes from outside the cluster to all routers in the cluster. Routers in a cluster do not need to be fully meshed.
router link advertisement	OSPF link-state advertisement flooded throughout a single area by all routers to describe the state and cost of the router's links to the area.
routing domain	<i>See AS.</i>
Routing Engine	Architectural portion of the router that handles all routing protocol processes, as well as other software processes that control the router's interfaces, some of the chassis components, system management, and user access to the router.
routing instance	A collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables and the routing protocol parameters control the information in the routing tables.
routing table	Common database of routes learned from one or more routing protocols. All routes are maintained by the JUNOS routing protocol process.
RP	For PIM-SM, a core router acting as the root of the distribution tree in a shared tree.
rpd	JUNOS software routing protocol process (daemon). User-level background process responsible for starting, managing, and stopping the routing protocols on a Juniper Networks router.
RPM	Reverse path multicasting. Routing algorithm used by DVMRP to forward multicast traffic.
RSVP	Resource Reservation Protocol. Resource reservation setup protocol designed to interact with integrated services on the Internet.

S

SA	Security association. An IPSec term that describes an agreement between two parties about what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications.
SAP	Session Announcement Protocol. Used with multicast protocols to handle session conference announcements.
SAR	Segmentation and reassembly. Buffering used with ATM.
SCB	System Control Board. On an M40 router, the part of the Packet Forwarding Engine that performs route lookups, monitors system components, and controls FPC resets.
SCG	SONET Clock Generator. Provides Stratum 3 clock signal for the SONET/SDH interfaces on the router. Also provides external clock inputs.
SDH	Synchronous Digital Hierarchy. CCITT variation of SONET standard.
SDP	Session Description Protocol. Used with multicast protocols to handle session conference announcements.
SDRAM	Synchronous dynamic random access memory.
Secure Hash Algorithm	<i>See SHA-1.</i>
secure shell	<i>See SSH.</i>

security association	<i>See SA.</i>
Security Parameter Index	<i>See SPI.</i>
SFM	Switching and Forwarding Module. On an M160 router, a component of the Packet Forwarding Engine that provides route lookup, filtering, and switching to FPCs.
SHA-1	Secure Hash Algorithm. A widely used hash function for use with Digital Signal Standard (DSS). SHA-1 is more secure than MD5.
shortest-path-first algorithm	<i>See SPF.</i>
signaled path	In traffic engineering, an explicit path; that is, a path determined using RSVP signaling. The ERO carried in the packets contains the explicit path information.
SIB	Switch Interface Board. Provides the switching function to the destination Packet Forwarding Engine.
simplex interface	An interface that assumes that packets it receives from itself are the result of a software loopback process. The interface does not consider these packets when determining whether the interface is functional.
SNMP	Simple Network Management Protocol. Protocol governing network management and the monitoring of network devices and their functions.
SONET	Synchronous Optical Network. High-speed (up to 2.5 Gbps) synchronous network specification developed by Bellcore and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988. <i>See also SDH.</i>
SPF	Shortest-path first, an algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links. Also called the <i>Dijkstra algorithm</i> .
SPI	Security Parameter Index. A portion of the IPSec Authentication Header that communicates which security protocols, such as authentication and encryption, are used for each packet in a VPN connection.
SPQ	Strict Priority Queuing. Dequeuing method that provides a special queue that is serviced until it is empty. The traffic sent to this queue tends to maintain a lower latency and more consistent latency numbers than traffic sent to other queues. <i>See also APQ.</i>
SSB	System and Switch Board. On an M20 router, Packet Forwarding Engine component that performs route lookups and component monitoring and monitors FPC operation.
SSH	Secure shell. Software that provides a secured method of logging in to a remote network system.
SSRAM	Synchronous Static Random Access Memory.
static LSP	<i>See static path.</i>
static path	In the context of traffic engineering, a static route that requires hop-by-hop manual configuration. No signaling is used to create or maintain the path. Also called a <i>static LSP</i> .
STM	Synchronous Transport Module. CCITT specification for SONET at 155.52 Mbps.

strict	In the context of traffic engineering, a route that must go directly to the next address in the path. (Definition from RFC 791, modified to fit LSPs.)
STS	Synchronous Transport Signal. Synchronous Transport Signal level 1. Basic building block signal of SONET, operating at 51.84 Mbps. Faster SONET rates are defined as STS- <i>n</i> , where <i>n</i> is a multiple of 51.84 Mbps. <i>See also</i> SONET.
stub area	In OSPF, an area through which, or into which, AS external advertisements are not flooded.
subnet mask	Number of bits of the network address used for host portion of a Class A, Class B, or Class C IP address.
summary link advertisement	OSPF link-statement advertisement flooded throughout the advertisement's associated areas by area border routers to describe the routes that they know about in other areas.
sysid	System identifier. Portion of the ISO nonclient peer. The sysid can be any 6 bytes that are unique throughout a domain.
System and Switch Board	<i>See</i> SSB.
T	
TACACS+	Terminal Access Controller Access Control System Plus. Authentication method for validating users who attempt to access the router using Telnet.
TCP	Transmission Control Protocol. Works in conjunction with Internet Protocol (IP) to send data over the Internet. Divides a message into packets and tracks the packets from point of origin to destination.
ToS	Type of service. The method of handling traffic using information extracted from the fields in the ToS byte to differentiate packet flows.
traffic engineering	Process of selecting the paths chosen by data traffic in order to balance the traffic load on the various links, routers, and switches in the network. (Definition from http://www.ietf.org/internet-drafts/draft-ietf-mpls-framework-04.txt .) <i>See also</i> MPLS.
transit area	In OSPF, an area used to pass traffic from one adjacent area to the backbone or to another area if the backbone is more than two hops away from an area.
transit router	In MPLS, any intermediate router in the LSP between the ingress router and the egress router.
transport mode	An IPSec mode of operation in which the data payload is encrypted, but the original IP header is left untouched. The IP addresses of the source or destination can be modified if the packet is intercepted. Because of its construction, transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. VPN gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. <i>See also</i> tunnel mode.
Triple-DES	A 168-bit encryption algorithm that encrypts data blocks with three different keys in succession, thus achieving a higher level of encryption. Triple-DES is one of the strongest encryption algorithms available for use in VPNs.
tunnel	Private, secure path through an otherwise public network.

tunnel mode An IPsec mode of operation in which the entire IP packet, including the header, is encrypted and authenticated and a new VPN header is added, protecting the entire original packet. This mode can be used by both VPN clients and VPN gateways, and protects communications that come from or go to non-IPsec systems. *See also transport mode.*

Tunnel PIC A physical interface card that allows the router to perform the encapsulation and decapsulation of IP datagrams. The Tunnel PIC supports IP-IP, GRE, and PIM register encapsulation and decapsulation. When the Tunnel PIC is installed, the router can be a PIM rendezvous point (RP) or a PIM first-hop router for a source that is directly connected to the router.

type of service *See ToS.*

U

unicast Operation of sending network traffic from one network node to another individual network node.

UPS Uninterruptible power supply. Device that sits between a power supply and a router (or other piece of equipment) that prevents undesired power-source events, such as outages and surges, from affecting or damaging the device.

V

vapor corrosion inhibitor *See VCI.*

VCI Vapor corrosion inhibitor. Small cylinder packed with the router that prevents corrosion of the chassis and components during shipment.

VCI Virtual circuit identifier. 16-bit field in the header of an ATM cell that indicates the particular virtual circuit the cell takes through a virtual path. Also called a *logical interface*. *See also VPI.*

virtual circuit identifier *See VCI.*

virtual link In OSPF, a link created between two routers that are part of the backbone but are not physically contiguous.

virtual path identifier *See VPI.*

virtual private network *See VPN.*

Virtual Router Redundancy Protocol *See VRRP.*

VPI virtual path identifier. 8-bit field in the header of an ATM cell that indicates the virtual path the cell takes. *See also VCI.*

VPN virtual private network. A private data network that makes use of a public TCP/IP network, typically the Internet, while maintaining privacy with a tunneling protocol, encryption, and security procedures.

VRRP Virtual Router Redundancy Protocol. On Fast Ethernet and Gigabit Ethernet interfaces, allows you to configure virtual default routers.

W

wavelength-division multiplexing *See WDM.*

WDM Wavelength-division multiplexing. Technique for transmitting a mix of voice, data, and video over various wavelengths (colors) of light.

WFQ Weighted Fair Queuing.

weighted round-robin *See WRR.*

WRR Weighted round-robin. Scheme used to decide the queue from which the next packet should be transmitted.

Part 9

Index

- Index on page 435
- Index of Statements and Commands on page 451

Index

Symbols

regular expression operator.....	112, 258, 260
wildcard	184
" ", configuration group wildcards	184
#	
comment delimiter.....	167
configuration mode prompt	136
#, in configuration statements.....	xxxiii
\$, regular expression operator.....	112, 258, 260
()	
in syntax descriptions	xxxiii
regular expression operator.....	112, 258, 260
*	
regular expression operator.....	260
*, wildcard character	184
+	
regular expression operator.....	260
+, in statement lists.....	137
-, wildcard character	184
.	
regular expression operator.....	260
/* */, comment delimiters	167
< >	
in syntax descriptions	xxxii
wildcard patterns	184
>	
CLI prompt.....	101
in statement lists.....	137
?	
wildcard	184
[]	
banners.....	136
in configuration statements.....	xxxiii
regular expression operator.....	112, 258, 260
[, wildcard	184
], wildcard	184
^	
regular expression operator.....	112, 258, 260
{ }	
in configuration statements.....	xxxiii
specifying statements.....	176

(pipe).....	110
filtering command output	217
in syntax descriptions	xxxiii
(pipe) command	217

A	
access permission bit.....	255
access privilege levels	
entering configuration mode	131
login classes	254
permission bits.....	255
user accounts	263
See also security	
access-control permission bit.....	255
accounting-options statement	
usage guidelines	137
activate command	203
usage guidelines	166
addresses	
IP addresses	235
router source addresses.....	278, 292
admin permission bit.....	255
admin-control permission bit.....	255
aggregated devices, configuring.....	381
aggregated-devices statement	397
usage guidelines	381
alarm conditions	
chassis alarm conditions	383
PIC alarms.....	382
silencing alarm devices	384
alarm cutoff button.....	384
alarm statement.....	398
usage guidelines	382
alert (system logging severity level)	273
alias statement	
usage guidelines	234
all permission bit.....	255
allow-commands statement	285
usage guidelines	256
allow-configuration statement	286
usage guidelines	256
allowing commands to login classes	256
/altconfig directory.....	225

•	alternate boot device	78
•	alternative media alarm condition	383
•	/altroot directory	225
•	annotate command	204
•	usage guidelines	167
•	any (system logging facility)	272
•	apply-groups statement	195
•	usage guidelines	180
•	archive option	273
•	archiving system logs	273
•	ATM	21, 32
•	ATM interfaces	
•	PIC alarm conditions	382
•	atm-cell-relay-accumulation statement	398
•	auditing for security	20
•	authentication	
•	diagnostics port	284
•	diagnostics port password	295
•	local user fallback mechanism	250
•	NTP authentication keys	269
•	order	248, 323
•	protocol	226
•	RADIUS	227, 241, 245, 249
•	root password	239
•	shared user accounts	245, 249
•	TACACS+	227, 243, 245
•	user accounts	263
•	user authentication	227
•	<i>See also</i> passwords; security	
•	authentication algorithm (IKE)	
•	usage guidelines	345
•	authentication method (IKE)	
•	usage guidelines	345
•	authentication order statement	325
•	authentication statement	286, 361
•	usage guidelines	262
•	authentication-algorithm (IKE) statement	362
•	authentication-algorithm (IPSec) statement	362
•	authentication-algorithm statement	362
•	authentication-key statement	287
•	usage guidelines	269
•	authentication-method statement	363
•	authentication-order statement	287
•	usage guidelines	248, 323
•	authorization (system logging facility)	272, 274
•	auxiliary port	15
•	properties	277
•	auxiliary statement	288
•	usage guidelines	277

B	backing up root file system	158
•	backup routers	237, 288
•	backup Routing Engine	393
•	backup-router statement	288
•	usage guidelines	237

banners	136
BGP routing protocol	10, 21
bgp statement	
usage guidelines	46
boot devices	78
boot sequences	79
boot server, NTP	267
boot-server statement	289
usage guidelines	267
braces, in configuration statements	xxxiii
brackets	
angle, in syntax descriptions	xxxii
square, in configuration statements	xxxiii
broadcast messages, synchronizing NTP	290
broadcast mode	
NTP	267, 269
broadcast statement	289
usage guidelines	269
broadcast, synchronizing NTP	270
broadcast-client statement	290
usage guidelines	270
bundles	75

candidate configurations	158
ce1 statement	399
certificates	
usage guidelines	360
certificates statement	363
Challenge Handshake Authentication Protocol	
usage guidelines	322
change-log (system logging facility)	272
channel-group statement	399
channelized DS-3 to DS-0 naming	386
channelized E1 naming	388
channelized mode	385
CHAP	22
chassis	
configuration	
alarm conditions	382
channelized PIC operation	385
configuration statements	379
drop policies	390
redundancy properties	390
SONET/SDH framing	384
process	14
chassis statement	36, 399
usage guidelines	137, 379
class statement	290
usage guidelines	253, 262
class-of-service statement	37
usage guidelines	137
clear command	215
usage guidelines	103
clear permission bit	255

- CLI..... 102
 - command completion..... 102
 - command history..... 120
 - comparing configuration versions..... 114
 - configuration mode *See* configuration mode, CLI
 - date, setting..... 119
 - editing command line..... 108
 - environment settings..... 123
 - filtering command output..... 110
 - hierarchy of commands..... 102, 145
 - keyboard sequences..... 108, 109
 - logging CLI command activity..... 273, 275
 - messages..... 107
 - modes..... 101
 - More-- prompt..... 109
 - operational mode *See* operational mode
 - overview..... 15, 101
 - prompt strings..... 101, 124
 - screen output..... 109
 - type checking..... 178
 - typing commands..... 101
 - users, monitoring..... 121
- client mode, NTP..... 267, 268
- command hierarchy..... 102, 145
- command history
 - configuration mode..... 156
 - operational mode..... 120
- command output
 - configuration details..... 116
 - counting lines..... 116
 - displaying all output..... 116
 - filtering..... 110
 - More-- prompt..... 109
 - multiple filters..... 119
 - retaining..... 116
 - saving to files..... 111
 - string searches..... 112
- command-line interface *See* CLI
- commands
 - allowing or denying to login classes..... 256
 - command line *See* CLI
 - completion..... 125, 139
 - configuration mode..... 139
 - configure..... 125
 - filenames, specifying..... 224
 - help about commands..... 105, 141
 - hierarchy..... 102, 145
 - history..... 120, 156
 - logging CLI command activity..... 273, 275
 - output *See* command output
 - overview..... 103
 - running operational commands in
 - configuration mode..... 156
 - typing..... 101
 - URLs, specifying..... 224
- comments..... 167
 - in configuration statements..... xxxiii
- commit and-quit command..... 205
 - usage guidelines..... 158
- commit check command..... 205
 - usage guidelines..... 157, 158
- commit command..... 205
 - usage guidelines..... 157, 164
- commit confirmed command..... 205
 - usage guidelines..... 158
- commit synchronize command..... 205
 - usage guidelines..... 160
- committing configurations
 - exiting configuration mode..... 158
 - previously committed configurations..... 164
 - usage guidelines..... 157
- compare command
 - usage guidelines..... 114
- comparing configuration versions..... 114
- compress-configuration-files statement..... 291
 - usage guidelines..... 240
- compressing configuration files..... 240, 291
- concatenated mode..... 385
- /config directory..... 85, 130, 225
- configuration files
 - compressing..... 240, 291
 - copying..... 391
 - saving to files..... 161
- configuration groups
 - applying..... 180
 - copying configuration files..... 391
 - creating..... 180, 181, 196
 - example configuration groups..... 187
 - inheritance model..... 180
 - inherited values..... 183
 - interface parameters..... 189
 - nested groups..... 182
 - overview..... 179
 - peer entities..... 191
 - re0, re1 groups..... 181
 - regional configurations..... 193
 - sets of statements..... 187
 - wildcards..... 184, 194
 - See also* configurations
- configuration mode, CLI..... 157
 - +..... 137
 - >..... 137
 - banners..... 136
 - command completion..... 139
 - command history..... 156
 - commands..... 33
 - copying configuration statements..... 152
 - copying configurations..... 85
 - displaying current configuration..... 148
 - entering configuration mode..... 131
 - error messages..... 107, 165
 - example configurations..... 170
 - exiting configuration mode..... 148
 - loading configurations..... 162

- locking configurations 132
 - overview 101
 - prompt 136
 - running operational mode commands 156
 - statements *See* configuration statements
 - top-level statements 137
 - users editing configurations
 - displaying 150
 - multiple simultaneous users 170
 - verifying configurations 157
 - *See also* configurations
 - configuration statements
 - copying 152
 - deactivating 166
 - filenames, specifying 224
 - IP addresses, specifying 223
 - overview 136
 - reactivating 166
 - removing 150
 - sets of statements 187
 - specifying 176
 - statement hierarchy 34, 128, 145
 - symbols, including in statements 137
 - top-level statements 137
 - URLs, specifying 224
 - *See also* configuration mode, CLI; configurations
 - configurations
 - activate 157
 - aggregated devices 381
 - combining 162
 - comments 167
 - committing 157
 - comparing configuration versions 114
 - copying configurations 85
 - copying statements 152
 - creating 142
 - deactivating statements and identifiers 166
 - displaying configuration details 116
 - displaying current 148
 - displaying current configuration 148
 - groups *See* configuration groups
 - identifiers 136, 153, 176
 - initial router configuration 81
 - loading 162
 - locking 132
 - modifying 142
 - previously committed configurations 164
 - reactivating statements and identifiers 166
 - removing statements 150
 - replacing 162
 - saved configurations 130
 - saving to files 161
 - statements *See* configuration statements
 - storing 130
 - symbols, including in statements 137
 - verifying 157
 - *See also* configuration mode, CLI
 - configure command **215**
 - usage guidelines 104, 131
 - configure exclusive command **215**
 - usage guidelines 132
 - configure permission bit 255
 - configure private command 133, **215**
 - configure traffic
 - traffic overview
 - IPSec 356
 - configuring JUNOS software *See* configurations
 - conflict-log (system logging facility) 272
 - connections statement **49**
 - console port 15
 - properties 277
 - console statement **291**
 - usage guidelines 277
 - container statements 128
 - control permission bit 255
 - conventions, documentation xxxii
 - copy command **206**
 - usage guidelines 103, 152
 - copying configuration files 391
 - copying configurations 85
 - copying statements in configurations 152
 - core dump files
 - usage guidelines 284
 - counting output lines
 - usage guidelines 116
 - craft interface
 - alarm conditions 382, 384
 - alarm cutoff button 384
 - critical (system logging severity level) 273
 - cron (system logging facility) 272, 274
 - ct3 statement **400**
 - usage guidelines 386
 - curly braces, in configuration statements xxxiii
 - cursor, moving 108
 - customer support, contacting xxxv
- D**
- daemon (system logging facility) 272, 274
 - data types, CLI 178
 - date
 - setting from NTP servers 200
 - date, setting 119
 - deactivate command **206**
 - usage guidelines 166
 - deactivating statements and identifiers 166
 - debug (system logging severity level) 273
 - default-address-selection statement **292**
 - usage guidelines 278
 - delete command **207**
 - usage guidelines 150
 - deny-commands statement **292**
 - usage guidelines 256

deny-configuration
 usage guidelines 256
 deny-configuration statement **293**
 denying commands to login classes 256
 destination option 237, 288
 device-count statement **400**
 usage guidelines 381
 DHCP relay agents 279, 294
 dhcp-relay statement **294**
 usage guidelines 279
 dh-group statement **363**
 usage guidelines 346
 diagnostics port password 284, 295
 diag-port-authentication statement **295**
 usage guidelines 284
 direction statement **364**
 usage guidelines 340
 directories, JUNOS software 225
 disable statement
 usage guidelines 166
 disabling software processes 283
 display detail command
 usage guidelines 116
 display inheritance command
 usage guidelines 183
 displaying all command output 116
 displaying configuration details 116
 displaying current configuration 148
 displaying environment settings 125
 displaying users editing configuration 150
 Distributed Buffer Manager ASIC 5
 distribution components, JUNOS software 75
 DNS name servers, configuring 236
 documentation conventions xxxii
 domain names on routers 235
 domain-name statement **295**
 usage guidelines 235
 domains to be searched 236, 296
 domain-search statement **296**
 usage guidelines 236
 downloading software packages 90
 drop policies 390
 DS-1 interfaces, PIC alarm conditions 383
 DVMRP
 routing protocol 11
 tracing operations 324, 326, 354, 375
 dvmrp statement **49**
 dynamic security associations 344
 usage guidelines 343, 344
 dynamic statement **364**
 usage guidelines 343

E
 e1 statement **400**
 usage guidelines 388
 E3 interfaces
 PIC alarm conditions 383
 edit command **207**
 usage guidelines 143, 146
 edit permission bit 255
 editing command line 108
 Emacs keyboard sequences 108
 emergency (system logging severity level) 273
 encrypted passwords 239
 encrypted-password option 239
 encryption statement **365**
 usage guidelines 342
 encryption-algorithm statement (IKE) **366**
 usage guidelines 346
 encryption-algorithm statement (IPSec) **366**
 usage guidelines 350
 environment settings, CLI
 command completion 125
 configuring 123
 displaying settings 125
 example configuration 125
 idle timeout 124
 prompt string 124
 restarting after software upgrade 125
 screen dimensions 124
 terminal type 124
 environment, CLI
 date setting from NTP servers 200
 time setting from NTP servers 200
 error (system logging severity level) 273
 error messages
 CLI 107, 165
 ES PIC 354
 Ethernet 32
 Ethernet interfaces
 PIC alarm conditions 383
 Ethernet management port 15
 ethernet statement **401**
 usage guidelines 381
 exit command **208**
 usage guidelines 146, 148
 exit configuration-mode command **208**
 usage guidelines 148
 export policies 13

F
 facilities, system logging 272, 274
 facility-override statement **312**
 usage guidelines 274
 failover on-loss-of-keepalives statement
 usage guidelines 393
 failover statement **305, 401**
 usage guidelines 284

failover, configuring	284
fan alarm conditions	383
FEB alarm condition	383
field permission bit	255
file command	103, 215
file copy command	
usage guidelines	391
file system, backing up	158
filenames, specifying in commands	224
files	
configuration files, compressing	240, 291
configuration files, copying	391
saving command output	111
saving configurations to files	161
filtering command output	110
	116
(pipe)	110
comparing configuration versions	114
displaying all output	116
multiple filters	119
retaining output	116
saving to files	111
string searches	112
finger access	280
finger service, configuring	280
finger statement	310
usage guidelines	280
firewall (system logging facility)	272
firewall filters	20
firewall permission bit	255
firewall statement	38
usage guidelines	137
firewall-control permission bit	255
flash drives	
mirroring to hard drives	238
storage media overview	78
floppy permission bit	255
forwarding table	12
forwarding-options statement	38
usage guidelines	138
FPC alarm condition	384
fpc statement	402
usage guidelines	385
Frame Relay	22, 32
framing modes	384
framing statement	403
usage guidelines	384
FTP service, configuring	281
ftp statement	
usage guidelines	281
full names, in user accounts	263
full-name statement	296
usage guidelines	262

global tracing operations	225
GMPLS	22
GRE encapsulation	23
groups statement	40, 196
usage guidelines	138, 180, 181

hard drives	
mirroring flash drives	238
storage media overview	78
hardware components.....	3
help apropos command.....	208
usage guidelines.....	141
help command.....	208
usage guidelines.....	141
help reference command.....	208
usage guidelines.....	141
hierarchy	
CLI commands	102, 145
configuration statements.....	34, 128, 145
history, CLI commands	
configuration mode.....	156
operational mode.....	120
HMAC-MD5 authentication	226
hold command	
usage guidelines.....	116
host-name statement.....	296
usage guidelines.....	233
hot-swapping alarm condition	384

ICMP routing protocol	10
identifiers	
deactivating.....	166
inserting in sequential lists	153
reactivating	166
renaming	153
specifying.....	176
idle timeout values	
CLI sessions.....	124
login classes	262
idle-timeout statement.....	297
usage guidelines.....	262
IGMP routing protocol	11
igmp statement.....	50

- IKE 331, 344
 - authentication algorithm
 - usage guidelines 345
 - authentication method
 - usage guidelines 345
 - DH group
 - usage guidelines 346
 - dynamic SAs 344
 - encryption-algorithm statement
 - usage guidelines 346
 - global properties
 - usage guidelines 344
 - lifetime
 - usage guidelines 346
 - mode
 - usage guidelines 348
 - policy
 - example 349
 - usage guidelines 347
 - preshared key statement
 - usage guidelines 348
 - proposal
 - usage guidelines 345, 348
 - proposal properties
 - usage guidelines 344
- ike statement **366**
 - usage guidelines 344
- import policies 13
- inactive tag 166
- inet statement **311**
 - usage guidelines 234
- info (system logging severity level) 273
- inheritance model, configuration groups 180
- inherited values, configuration groups 183
- insert command **209**
 - usage guidelines 153
- installing JUNOS software
 - factory installation 75
 - initial router configuration 81
 - naming conventions 76
 - overview 15
 - package names 76
 - reconfiguring 86
 - release names 76
 - software distribution components 75
 - storage media 78
 - See also* JUNOS software
- interactive-commands (system logging facility) 272, 273
- interface
 - media parameters 189
 - permission bit 255
 - process 14
 - tracing operations 226
- interface statement **298**
 - usage guidelines 279
- interface-control permission bit 255
- interfaces statement
 - usage guidelines 138
- Internet drafts supported 21
- Internet Key Exchange, *See* IKE
- Internet Processor ASIC 6
- IP
 - multicast 23
 - packets, router source addresses 278, 292
 - traffic, discarding 390
- IP addresses 223, 234
 - router mapping 235
 - router names, mapping 234
 - specifying in statements 223
- IP-IP encapsulation 23
- IPSec
 - authentication
 - usage guidelines 341
 - authentication algorithm
 - usage guidelines 350
 - direction
 - usage guidelines 340
 - dynamic security associations 344
 - usage guidelines 343
 - encryption
 - usage guidelines 342
 - encryption-algorithm statement
 - usage guidelines 350
 - ES PIC 354
 - example, configure inbound traffic 358
 - example, configure outbound traffic 357
 - global properties 336
 - IKE 331
 - lifetime of SA
 - usage guidelines 351
 - minimum configurations
 - dynamic SA 335
 - IPSec 335
 - manual SA 335
 - mode
 - usage guidelines 338
 - overview 329
 - perfect-forward-secrecy statement
 - usage guidelines 352
 - policy 352
 - overview 352
 - usage guidelines 352
 - proposal
 - usage guidelines 350
 - proposal properties 336
 - protocol (manual SA)
 - usage guidelines 341
 - protocol for dynamic SA
 - usage guidelines 351
 - replay window size
 - usage guidelines 339

• security associations	330
• security parameter index	
• usage guidelines.....	341
• security services overview.....	329
• traffic	355
• types of security.....	330
• ipsec statement.....	367
• usage guidelines.....	336
• IS-IS routing protocol.....	10, 25, 31
• isis statement	
• usage guidelines.....	50
• ISO standards supported	31
• issue relative configuration commands	147

J juniper.conf file, compressing	240, 291
• Juniper-Allow-Commands attribute.....	242, 244
• Juniper-Allow-Configuration attribute	242, 244
• Juniper-Deny-Commands attribute.....	242, 244
• Juniper-Deny-Configuration attribute.....	242, 244
• Juniper-Local-User-Name attribute.....	242, 244
• JUNOS software	
• boot sequence.....	79
• configuration overview.....	16
• directories stored in	225
• factory installation	75
• initial router configuration.....	81
• installation	15
• naming conventions.....	76
• package names	76
• reconfiguring.....	86
• release names.....	76
• software distribution components.....	75
• standards supported	21
• storage media	78
• JUNOScript xml-ssl service	360

K keepalive-time statement.....	403
• usage guidelines.....	393
• kernel (system logging facility)	272, 274
• kernel, Routing Engine	15
• keyboard sequences	
• editing command line	108
• --More-- prompt.....	109

L LDP	11, 25
• ldp statement.....	52
• leaf statement	128
• lifetime-seconds statement (IKE)	368
• usage guidelines.....	346
• lifetime-seconds statement (IPSec)	368
• usage guidelines.....	351
• lo0 interface	278, 292
• load command.....	209
• usage guidelines.....	162
• load replace command.....	392
• load-key-file command	298
• usage guidelines.....	239, 262
• local password authentication	245
• local user	
• fallback mechanism	250
• template accounts	246
• template example	246
• local0–local7 (system logging facilities)	274
• location statement.....	299
• usage guidelines.....	238
• locking configurations	132
• log files redundancy logging	390
• logging in as root.....	282
• logging operations	
• system logging	271, 275
• tracing operations	225
• logical devices	381
• login classes	
• access privilege levels.....	254
• commands, allowing or denying	256
• default classes	256
• defining.....	253, 256
• idle timeout values	262
• login messages, system	283
• login statement	300
• usage guidelines.....	253, 262
• log-prefix statement	313
• usage guidelines.....	275

M maintenance permission bit	255
• management Ethernet interface	
• PIC alarm conditions	383
• management process	15
• managing routers <i>See</i> SNMP	
• manual security association.....	339
• manual statement	368
• match command	
• usage guidelines.....	112

maximum-hop-count statement **298**
 usage guidelines 279
 MD5 authentication 226
 merge option 162
 message statement **300**
 usage guidelines 283
 messages
 broadcast messages, NTP 270, 290
 CLI 107
 error 165
 logging *See* system logging
 multicast, NTP 270
 redirect 278
 system login 283
 MIB II process 14
 MIBs standards supported 26
 minimum-wait-time statement **298**
 usage guidelines 279
 mirror-flash-on-disk statement **301**
 usage guidelines 238
 mode statement **369**
 modifying configurations 142
 monitor command 103, **216**
 monitoring tools
 overview 17
 system logging 271, 275
 tracing operations 225
 See also MIBs; SNMP
 --More-- prompt 109
 MPLS protocol 11
 supported Internet standards and 28
 MPLS routing table 12
 mpls statement
 usage guidelines 52
 MSDP routing protocol 11
 msdp statement
 usage guidelines 55
 m-series routers 5
 multicast
 NTP
 messages 270
 routing protocols 11
 routing table 12
 multicast-client statement **301**
 usage guidelines 270
 multiplexed mode 385

N
 name servers, DNS 236
 names
 domain names on routers 235
 package 76
 release 76
 router 233, 234
 router names 235
 wildcard 194

name-server statement **302**
 usage guidelines 236
 neighbor discovery
 configuration statements 59
 nested configuration groups 182
 network
 masks 223
 permission bit 255
 Network Time Protocol *See* NTP
 no 298
 no-concatenate statement **404**
 usage guidelines 385
 no-listen statement 279, **298**
 usage guidelines 279
 no-more command **217**
 usage guidelines 116
 non-concatenated mode 385
 no-packet-scheduling statement **404**
 usage guidelines 395
 no-redirects statement **302**
 usage guidelines 278
 no-saved-core-context statement **302**
 usage guidelines 284
 no-source-route statement **408**
 usage guidelines 390
 notice (system logging severity level) 273
 NTP
 authentication keys 269
 boot server 267
 broadcast mode 267, 269
 client mode 267, 268
 configuring 266
 listening for broadcast messages 270, 290
 listening for multicast messages 270
 set date ntp 119
 symmetric active mode 267, 268
 ntp statement **303**
 usage guidelines 266

O

operational mode
 command history 120
 command overview 103
 date, setting 119
 running commands in configuration mode 156
 users, monitoring 121
 operator login class 256
 operators, regular expression 112, 258, 260
 OSPF
 routing protocol 10
 standards supported 28
 ospf statement **56**
 output of commands *See* command output
 override option 162
 overriding system logging facilities 274

P

- packages 75, 76, 90
 - transferring between Routing Engines 393
- Packet Forwarding Engine..... 5
- packet scheduling..... 395
- packets
 - flow through routers..... 5
 - router source addresses 278, 292
- packet-scheduling statement..... **404**
 - usage guidelines 395
- passwords
 - diagnostics port..... 295
 - diagnostics port password..... 284
 - RADIUS authentication..... 241
 - root 239
 - shared user 245
 - shared user accounts..... 249
 - user accounts 263
- peer entities 191
- peer statement **303**
 - usage guidelines 268
- perfect-forward-secrecy statement **370**
 - usage guidelines 352
- permission bits..... 255
- permissions statement **304**
 - usage guidelines 254
- pfe (system logging facility) 272
- physical devices, aggregating 381
- physical interfaces, framing modes 384
- PIC alarm conditions 382
- pic statement..... **405**
 - usage guidelines 385
- PIM
 - routing protocol 11
- pim statement
 - usage guidelines 57
- ping command **216**
 - usage guidelines 103
- pipe (|)
 - filtering command output **217**
 - usage guidelines 110
 - in syntax descriptions xxxiii
- plain-text passwords 239
- plain-text-password option..... 239
- policy statement (IKE)
 - usage guidelines 347
- policy statement (IPSec and IKE)..... **370**
- policy statement (IPSec)
 - usage guidelines 352
- policy-options statement..... **46**
 - usage guidelines 138
- port statement **304, 405**
 - usage guidelines 241
- ports
 - auxiliary port properties 277
 - console port properties 277
 - diagnostics port..... 284, 295
 - external ports..... 15
 - RADIUS server port 241
- ports statement..... **304**
 - usage guidelines 277
- power supply alarm conditions 383
- PPP 29
- prefixes
 - log message prefixes 275
 - specifying in statements..... 223
- pre-shared-key statement **371**
 - usage guidelines 348
- primary boot device 78
- privileges *See* access privilege levels
- processes
 - configuring failover 284, 305
 - disabling..... 283
- processes statement **305**
 - usage guidelines 283
- profile statement..... **325**
 - usage guidelines 322
- prompt strings
 - # 136
 - > 101
 - CLI 101, 124
 - configuration mode..... 136
 - More-- prompt..... 109
 - usage guidelines 136
- proposal statement (IPSec and IKE) **372**
- protocol statement (manual and dynamic tunnel SA)..... **373**
- protocols
 - authentication 226
 - redirect messages 278
- protocols statement..... **46**
 - usage guidelines 138
- protocol-specific tracing operations 225
- protocol-version statement 282, **306**
 - usage guidelines 306

Q

- quit command..... 104, **210, 217**

R

- RADIUS authentication 227, 241, 249
 - TACACS+ 245
- radius-server statement **306**
 - usage guidelines 241
- re0 configuration group 181
- re1 configuration group 181
- reactivating statements and identifiers 166
- read-only login class 256
- reconfiguring JUNOS software 86
- red alarm conditions 382
- redirect 278
- redrawing screen 109
- redundancy
 - backup routing engine 393
 - configuring failover 284, 305
 - logging 390
 - SFM 394
 - SSB 394
 - synchronize routing engines 160
- redundancy statement **406**
 - usage guidelines 394
- regional configurations 193
- regular expression operators 112, 258, 260
- relay agents, DHCP 279, 294
- release names 76
- releases, upgrading to 89
- remote
 - access, configuring 280
 - template account 245
 - user names 249
- removable media 78
- removing statements from configurations 150
- rename command **210**
 - usage guidelines 153
- renaming identifiers 153
- replace option 162
- replay-window-size statement **374**
 - usage guidelines 343
- request command **218**
 - usage guidelines 104
- request system command
 - usage guidelines 393
- request system logout pid pid_number 132
- request system snapshot command
 - usage guidelines 158
- request system software add package-name
 - validate command 91, 92
- request system software package-name
 - validate command 92
- reset permission bit
 - usage guidelines 255
- restart command **218**
 - usage guidelines 103
- restarting after software upgrade 125
- retaining command output 116

- retry statement **307**
 - usage guidelines 241
- RIP routing protocol 10, 29
- rip statement **58**
- rlogin service, configuring 281, 310
- rlogin statement **310**
 - usage guidelines 281
- rollback command **211**
 - usage guidelines 164
- rollback permission bit 255
- root file system, backing up 158
- root password 239
- root-authentication statement **307**
 - usage guidelines 239
- root-login statement **308**
 - usage guidelines 282
- route prefixes 223
- router 390
- router access 19
- router chassis
 - configuration
 - alarm conditions 382
 - channelized PIC operation 385
 - configuration statements 379
 - redundancy properties 390
 - SDH/SONET framing 384
- router security 17
 - auditing for security 20
 - default settings 18
 - firewall filters 20
 - router access 19
 - routing protocol security features 20
 - user authentication 19
- router software *See* software, JUNOS
- router-discovery statement
 - usage guidelines 59
- routers
 - backup 237
 - backup routers 288
 - boot devices 78
 - boot sequence 79
 - configuring *See* configurations
 - DHCP relay agents 279, 294
 - DNS name servers, configuring 236
 - domain names 235
 - domains to be searched 236, 296
 - failover, configuring 284, 305
 - hardware components 3
 - initial router software configuration 81
 - login classes 253
 - managing *See* SNMP
 - names
 - configuring 233, 235
 - mapping to IP addresses 234, 235
 - NTP 266
 - Packet Forwarding Engine 5
 - physical system location 238

ports	
auxiliary port properties.....	277
console port properties.....	277
diagnostics port.....	284, 295
RADIUS server port.....	241
redirect.....	278
root login, controlling.....	282
Routing Engine.....	7, 9
software processes, disabling.....	283
source addresses.....	278, 292
storage media.....	78
system services, configuring.....	280
time zone setting.....	265
user accounts.....	262
Routing Engines.....	14
backup.....	393
chassis	
process.....	14
kernel.....	15
management process.....	15
MIB II process.....	14
overview.....	7
redundancy.....	393
routing protocol process.....	10
SNMP process.....	14
software components.....	9
tty connections.....	390
routing instance	
routing options.....	61
routing permission bit.....	255
routing protocol process	
routing policy.....	13
routing protocols.....	10, 12
routing tables.....	12
routing protocol security features.....	20
routing protocols	
MPLS applications.....	11
multicast routing.....	11
overview.....	10
unicast.....	10
routing tables.....	12
routing-control permission bit.....	255
routing-engine statement.....	406
usage guidelines.....	390
routing-instances statement.....	60
usage guidelines.....	60, 138
routing-options statement.....	63
usage guidelines.....	61, 138
RSVP.....	11, 29
rsvp statement.....	59
run command.....	211
usage guidelines.....	156
running operational commands.....	156

S	sap statement	60
	SAP/SDP routing protocol	11
	save command	212
	usage guidelines	111, 161
	SCB alarm condition	383
	scheduling packets	395
	screen dimensions	124
	screen output <i>See</i> command output	
	screen, redrawing	109
	SDH	31
	SDH framing	384
	SDH interfaces	
	framing mode	384
	PIC alarm conditions	382
	sdp statement	60
	searching	
	regular expressions	112
	strings in command output	112
	secret permission bit	255
	secret statement	308
	RADIUS authentication	
	usage guidelines	241
	TACACS+ authentication	
	usage guidelines	243
	secret-control permission bit	255
	security	
	router port properties	278
	<i>See also</i> access privilege levels; authentication; passwords	
	security association statement	
	usage guidelines	337
	Security Services Configuration Guidelines	333
	security-association statement	374
	server statement	309
	usage guidelines	268, 279
	services statement	310
	usage guidelines	280
	set cli complete-on-space command	197
	usage guidelines	125
	set cli idle-timeout command	198
	usage guidelines	124
	set cli prompt command	198
	usage guidelines	124
	set cli restart-on-upgrade command	198
	usage guidelines	125
	set cli screen-length command	199
	usage guidelines	124
	set cli screen-width command	199
	usage guidelines	124
	set cli terminal command	199
	usage guidelines	124
	set command	213, 218
	usage guidelines	142
	set date and time from NTP servers	119
	set date command	200
	usage guidelines	119

- set date ntp command 119, **200**
- settings, CLI, displaying 125
- severity levels, system logging 273
- SFM alarm condition 383
- SFM redundancy 394
- sfm statement **407**
 - usage guidelines 394
- shared user accounts 249
- shell permission bit 255
- show cli command **200**
 - usage guidelines 125
- show cli history command **201**
 - usage guidelines 120
- show command 103, **213**, **218**
 - usage guidelines 147, 148
- show configuration command
 - usage guidelines 148
- simple authentication 226
- single-connection statement **311**
 - usage guidelines 243
- snmp permission bit 255
- SNMP process 14
- snmp statement
 - usage guidelines 138
- snmp-control permission bit 255
- software monitoring tools *See* monitoring tools
- software processes
 - configuring failover 284, 305
 - disabling 283
- software, JUNOS
 - boot sequence 79
 - configuration overview 16
 - directories stored in 225
 - factory installation 75
 - initial router configuration 81
 - installation 15
 - naming conventions 76
 - package names 76
 - reconfiguring 86
 - release names 76
 - software distribution components 75
 - standards supported 21
 - storage media 78
 - See also* SNMP
- SONET 31
 - framing 384
 - interfaces
 - framing mode 384
 - PIC alarm conditions 382
- sonet statement **407**
 - usage guidelines 381
- source-route constraints 390
- source-route statement **408**
 - usage guidelines 390
- sparse-dlci statement **409**
 - usage guidelines 385
- spi statement **374**
 - usage guidelines 341
- SSB alarm condition 383
- SSB redundancy 394
- ssb statement **408**
 - usage guidelines 394
- ssh command **219**
 - usage guidelines 103
- SSH key files 239
- ssh protocol version 282
- ssh service
 - configuring 281
 - root login 282
 - ssh protocol version 282
- ssh statement **310**
 - usage guidelines 281
- standards supported by software 21
- start command 104, **219**
- statement hierarchy 34, 128, 145
- statement paths 128
- statements
 - configuration mode statements 136
 - copying in configurations 152
 - deactivating 166
 - filenames, specifying 224
 - IP addresses, specifying 223
 - reactivating 166
 - removing from configurations 150
 - sets, in configuration groups 187
 - specifying 176
 - top-level statements 137
 - URLs, specifying 224
 - See also* configuration mode, CLI; configurations
- static statement
 - usage guidelines 237
- static-host-mapping statement **311**
 - usage guidelines 234
- status command **213**
 - usage guidelines 150
- storage media 78
- storing configurations 130
- strings, searching command output 112
- subnet masks 223
- super-user login class 256
- support, technical xxxv
- supported Internet RFCs and Drafts 21
- symmetric active mode, NTP 267, 268
- synchronize routing engines 160
- sysid statement **311**
 - usage guidelines 234
- syslog statement **312**
 - usage guidelines 271
- system
 - identifiers 234
 - login 283

•	system authentication	
•	authentication order.....	248
•	RADIUS authentication.....	241, 245, 249
•	TACACS+ authentication.....	243, 245
•	<i>See also</i> authentication	
•	system logging	
•	archiving system logs.....	273
•	CLI commands, logging.....	273, 275
•	configuring.....	271
•	example configuration	275
•	facilities.....	272, 274
•	log message prefixes.....	275
•	overriding facilities.....	274
•	severity levels	273
•	system permission bit	256
•	system services	
•	configuring on routers.....	280
•	rlogin service.....	281
•	ssh service	281
•	system services	
•	finger service	280
•	ftp service	281
•	telnet service.....	283
•	system statement.....	69, 313
•	usage guidelines.....	138, 229
•	system-control permission bit	256

T	t1 statement.....	409
•	T3	32
•	T3 interfaces	
•	PIC alarm conditions.....	383
•	TACACS+ authentication.....	227, 243, 245
•	tacplus-server statement.....	314
•	usage guidelines.....	243
•	TCP/IP v4	30
•	technical support.....	xxxv
•	telnet	
•	access, configuring.....	280
•	service, configuring.....	283
•	telnet command	219
•	usage guidelines.....	103
•	telnet statement.....	310
•	usage guidelines.....	283
•	temperature alarm conditions.....	383
•	template accounts	245, 249
•	template accounts for RADIUS and TACACS+ authentication.....	245
•	terminal	
•	option	162
•	terminal type.....	124, 278, 291
•	test command	219
•	usage guidelines.....	103
•	time	
•	setting from NTP servers.....	200
•	setting from the CLI	119

time zone setting, routers.....	265
timeout statement.....	314
RADIUS authentication	
usage guidelines.....	241
TACACS+ authentication	
usage guidelines.....	243
timeslots statement	409
usage guidelines	386
time-zone statement.....	315
usage guidelines	265
top command.....	147, 214
usage guidelines	147
top-level statements	137
trace access process usage guidelines.....	324
trace permission bit.....	256
trace-control permission bit.....	256
traceoptions statement	326
usage guidelines.....	35, 67, 321, 324, 334, 354, 375
traceroute command	219
usage guidelines	103
tracing operations	225
DVMRP	324, 326, 354, 375
<i>See also</i> logging operations	
traffic.....	355
inbound (decryption).....	358
outbound (encryption).....	357
trusted-key statement.....	317
usage guidelines	269
t-series routers.....	6
tty connections between routing engines	390
type checking, CLI.....	178
type statement.....	288, 291
usage guidelines	278
typefaces, documentation conventions	xxxii
typing commands	101

U	uid statement.....	317
•	usage guidelines	262
•	UIDs	263
•	unauthorized login class	256
•	unicast	
•	routing protocols.....	10
•	routing table.....	12
•	up command.....	147, 214
•	usage guidelines	146
•	update command	216
•	usage guidelines	135
•	update configure private configuration.....	135
•	upgrading software.....	89, 125
•	URLs, specifying in commands.....	224
•	usage guidelines	116
•	user (system logging facility)	272, 275

- user access
 - login classes 253
 - user accounts 262
- user accounts
 - authentication 263
 - configuring 262
 - shared user accounts 245, 249
- user authentication 19, 227, 263
 - See also* authentication
- user statement **318**
 - usage guidelines 262
- users editing configurations
 - displaying 150
 - multiple simultaneous users 170
- users of CLI, monitoring 121

V

- /var/db/config directory 130, 225
- /var directory 225
- /var/home directory 225
- /var/log directory 225
- /var/tmp directory 225
- view permission bit 256
- virtual links
 - aggregated devices 381
- VPNs 14

W

- warning (system logging severity level) 273
- wildcard names 194
- wildcards 184
- world-readable option 273

Y

- yellow alarm condition 382, 383

Index

Index of Statements and Commands

Symbols

(pipe)	
filtering command output	217
(pipe) command	217

A

activate command	203
aggregated-devices statement	397
alarm statement	398
allow-commands statement	285
allow-configuration statement	286
annotate command	204
apply-groups statement	195
atm-cell-relay-accumulation statement	398
authentication order statement	325
authentication statement	286, 361
authentication-algorithm (IKE) statement	362
authentication-algorithm (IPSec) statement	362
authentication-algorithm statement	362
authentication-key statement	287
authentication-method statement	363
authentication-order statement	287
auxiliary statement	288

B

backup-router statement	288
boot-server statement	289
broadcast statement	289
broadcast-client statement	290

C

ce1 statement	399
certificates statement	363
channel-group statement	399
chassis statement	399
class statement	290
clear command	215
commit and-quit command	205
commit check command	205
commit command	205

commit confirmed command	205
commit synchronize command	205
compress-configuration-files statement	291
configure command	215
configure exclusive command	215
configure private command	215
console statement	291
copy command	206
ct3 statement	400

D

deactivate command	206
default-address-selection statement	292
delete command	207
deny-commands statement	292
deny-configuration statement	293
device-count statement	400
dhcp-relay statement	294
dh-group statement	363
diag-port-authentication statement	295
direction statement	364
domain-name statement	295
domain-search statement	296
dynamic statement	364

E

e1 statement	400
edit command	207
encryption statement	365
encryption-algorithm statement (IKE)	366
encryption-algorithm statement (IPSec)	366
ethernet statement	401
exit command	208
exit configuration-mode command	208

F	facility-override statement	312
	failover statement	305, 401
	file command	215
	finger statement	310
	fpc statement	402
	framing statement	403
	full-name statement	296
H	help apropos command.....	208
	help command	208
	help reference command.....	208
	host-name statement.....	296
I	idle-timeout statement	297
	ike statement.....	366
	inet statement	311
	insert command	209
	interface statement	298
	ipsec statement.....	367
K	keepalive-time statement.....	403
L	lifetime-seconds statement (IKE)	368
	lifetime-seconds statement (IPSec)	368
	load command.....	209
	load-key-file command	298
	location statement	299
	login statement.....	300
	log-prefix statement	313
M	manual statement	368
	maximum-hop-count statement	298
	message statement	300
	minimum-wait-time statement.....	298
	mirror-flash-on-disk statement	301
	mode statement.....	369
	monitor command.....	216
	multicast-client statement.....	301
N	name-server statement.....	302
	no-concatenate statement.....	404
	no-listen statement.....	298
	no-more command	217
	no-packet-scheduling statement	404
	no-redirects statement.....	302
	no-saved-core-context statement	302
	no-source-route statement	408
	ntp statement	303
P	packet-scheduling statement	404
	peer statement.....	303
	perfect-forward-secrecy statement.....	370
	permissions statement.....	304
	pic statement.....	405
	ping command.....	216
	pipe () filtering command output	217
	policy statement (IPSec and IKE)	370
	port statement	304, 405
	ports statement.....	304
	pre-shared-key statement	371
	processes statement	305
	profile statement.....	325
	proposal statement (IPSec and IKE)	372
	protocol statement (manual and dynamic tunnel SA)	373
	protocol-version statement.....	306
Q	quit command	210, 217
R	radius-server statement	306
	redundancy statement.....	406
	rename command.....	210
	replay-window-size statement	374
	request command	218
	restart command	218
	retry statement	307
	rlogin statement.....	310
	rollback command	211
	root-authentication statement	307
	root-login statement	308
	routing-engine statement.....	406
	run command.....	211

S		U	
save command	212	uid statement	317
secret statement	308	up command	214
security-association statement	374	update command	216
server statement	309	user statement	318
services statement	310		
set cli complete-on-space command	197		
set cli idle-timeout command	198		
set cli prompt command	198		
set cli restart-on-upgrade command	198		
set cli screen-length command	199		
set cli screen-width command	199		
set cli terminal command	199		
set command	213, 218		
set date command	200		
set date ntp command	200		
sfm statement	407		
show cli command	200		
show cli history command	201		
show command	213, 218		
single-connection statement	311		
sonet statement	407		
source-route statement	408		
sparse-dlcis statement	409		
spi statement	374		
ssb statement	408		
ssh command	219		
ssh statement	310		
start command	219		
static-host-mapping statement	311		
status command	213		
sysid statement	311		
syslog statement	312		
system statement	313		
T			
t1 statement	409		
tacplus-server statement	314		
telnet command	219		
telnet statement	310		
test command	219		
timeout statement	314		
timeslots statement	409		
time-zone statement	315		
top command	214		
traceoptions statement	326		
traceroute command	219		
trusted-key statement	317		
type statement	288, 291		

